MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT
ENSM. Pôle Universitaire de KOLÉA

MEMOIRE DE FIN D'ETUDES

Master en Management Stratégique et Système d'information

Mise en place d'une démarche prospective de gestion des risques au sein de la Direction Informatique en utilisant la méthode MADS-MOSAR

Elaboré par : KHELIFI Adlene

Encadré par : Dr. CHOHRA Mohamed

Année 2017/2018

RÉSUMÉ

L'objectif principal de cette étude est d'assurer une gestion prospective du risque informatique à l'aider de la méthode MADS-MOSAR au sein de la Direction Informatique de la Direction Générale du Budget, plus précisément pour l'application de la méthode permit de mettre en œuvre une gestion d'anticipation des risques informatiques au sien de la Direction Informatique.

L'approche qualitative est utilisée pour répondre aux questions de recherche.

Les résultats ont démontré qu'il y a des insuffisances tout au long du processus, ce qui nous a permis de dégager des propositions, afin de l'améliorer pour garantir la qualité système informatique de la direction.

Mots clés : Prospective Stratégique – Système d'Information – Système Informatique -Risque Informatique – Gestion des Risques - MADS-MOSAR.

ABSTRACT

The main objective of this study is to ensure a forward-looking management of IT risk by using the MADS-MOSAR method within the IT Department of the Directorate General of Budget, more precisely for the application of the method allows to implement a management of anticipation of IT risks in the IT Department. The qualitative approach is used to answer research questions.

The results showed that there are shortcomings throughout the process, which allowed us to identify proposals, in order to improve it to guarantee the quality computer system of the management.

Key-words: Strategic perspective - Information system - Computer system - IT risk - Risk management - MADS-MOSAR.

ملخص

الهدف الرئيسي من هذه الدراسة هو ضمان إدارة استشرافية لمخاطر تكنولوجيا المعلومات باستخدام طريقة MADS-MOSAR في مديرية الإعلام الآلي بالمديرية العامة للميزانية، و بتعبير أدق تطبيق أسلوب يسمح بتنفيذ إدارة لتوقع مخاطر تكنولوجيا المعلومات في مديرية الإعلام الآلي.

يستخدم النهج النوعي للإجابة على أسئلة البحث.

أظهرت النتائج أن هناك أوجه قصور طوال العملية، مما سمح لنا بتحديد المقترحات، من أجل تحسينه ولضمان جودة في إدارة نظام الكمبيوتر للمديرية.

كلمات البحث: الاستشراف الاستراتيجي ـ نظام المعلومات ـ نظام تكنولوجيا المعلومات ـ مخاطر تكنولوجيا المعلومات ـ إدارة المخاطر MADS-MOSAR-

REMERCIEMENTS

Effectuer un travail synthétique d'analyse et de recherche en vue de faire le lien entre deux domaines n'est pas une tâche simple. Cela suppose une méthodologie, un regard neuf mais également des connaissances importantes sur le sujet traité. Dans le cadre de mes recherches, bien qu'ayant étudié dans une certaine mesure la prospective, ma connaissance de la gestion des risques était quant à elle parcellaire.

Je souhaite donc remercier les nombreuses personnes m'ayant guidé dans mes recherches, m'ayant reçu en entretien ou ayant accepté de répondre à mon enquête, afin de construire une approche aussi pertinente et complète que possible.

Ce mémoire est également l'occasion de remercier les différents intervenants de l'ENSM (Ecole Nationale Supérieur de Management), plus particulièrement **Dr. CHOHRA Mohamed** Professeur à l'ENSM et **Madame MESAID Amina** Directrices de l'école (ENSM), pour les nombreux éclairages apportés et l'ouverture sur un ensemble de domaines aussi variés qu'intéressants. Cette formation m'a beaucoup apporté, le regard prospectif est désormais structurant pour moi à de nombreux égards.

Je souhaite par ailleurs remercier tout particulièrement **Mr. BRAHIMI Farid**, Directeur d'informatique à la Direction Informatique de la Direction Générale du Budget, pour son intérêt pour mon domaine d'étude, ses nombreux conseils et son expertise.

Je souhaite encore adresser mes remerciements à **Mr. LAARI Ali**, Sous-directeur à la Direction Informatique de la Direction Générale du Budget pour ses conseils m'ayant permis d'améliorer ce mémoire.

Je voulais enfin remercier **Mr. HAMDAD Mohamed Lamine**, Chef de Bureau des systèmes d'informations à la Direction Informatiques de la Direction Générale du Budget, pour le vif intérêt accordé à mon domaine de recherche

Je voulais particulièrement remercier l'ensemble de mes camarades de la spécialité MSSI et plus particulièrement **HACHI Rafik**, pour les nombreuses réflexions menées dans plusieurs recherche de management stratégique et système d'information au cours des deux années d'études et de formation passer à l'ENSM, sources de synergies.

Sans ces différents regards, variés et attentifs, mon mémoire n'aurait pas la même contenance.

SOMMAIRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS

ENSM : École Nationale Supérieure De Management.

DGB : Direction Générale du Budget.

DI : Direction Informatique.

TIC : Technologies de l'information et de la communication.

ISO: International Organization for Standardization.

AMDEC : Analyse des Modes de Défaillance est des Effets Critiques.

MOSAR : Méthode Organisée et Systémique d'Analyse des Risques.

MADS : Modèle d'Analyse des Dysfonctionnements des Systèmes.

SI: Système d'Information.

COSO: Committee Of Sponsoring Organizations.

IVTS: Informal Value Transfer System.

IFACI : Institut français des auditeurs et contrôleurs internes

CLUSIF: Club de la Sécurité de l'Information Français

AMRAE: Association pour le Management des Risques et des Assurances en Entreprise

APSAD: Assemblée Plénière des Sociétés d'Assurance Dommage

CEA: Commissariat à l'Énergie Atomique

RSSI: Responsable de la Sécurité des Systèmes d'Information

ENASS: Ecole Nationale d'Assurances

CNAM: Conservatoire National des Arts et Métiers.

LIPSOR: Laboratoire d'Investigation en Prospective Stratégie et Organisation.

MAPROM: Méthode d'Analyse Prospective du Risque Opportunités et Menaces.

ENSAM : École nationale supérieure des arts et métiers.

HSE : hygiène sécurité environnement

INTRODUCTION

La période contemporaine s'inscrit plus que jamais dans un environnement à risques. Les « Mises en risque » opérée par les individus, consommateurs, entreprise, collectivités publiques vont croissantes et concernent désormais non simplement des risques majeurs redoutés mais des actions de la vie courante selon S.Cleary, T.Malleret (2006).

A cela s'ajoute la problématique des risques émergents, vecteurs de peurs mais également de prise de conscience de la nécessité d'anticiper plus que jamais les situations risqués.

Les systèmes d'information sont devenus l'outil incontournable dans les organisations publiques et ceux-ci suivent des cycles technologiques extrêmement rapides. De plus, les risques liés à l'utilisation de ces derniers sont devenus plus nombreux, significatifs et complexes. Par conséquent, une attention particulière doit leur être portée surtout en ce qui concerne l'évaluation, le contrôle et la surveillance de leurs dispositifs de maitrise des risques mis en place afin d'aider la direction à atteindre ses objectifs ; d'où la nécessité d'voir une prospection de gestion des risques selon PILLOU Jean-François et CAILLEREZ Pascal (2011).

C'est dans ce cadre que la gestion des risques, visant à la fois la réduction du coût des risques informatiques et la maîtrise de ces derniers, supportés par l'organisation, a évolué durant la seconde moitié du XXème siècle. Ce, d'une gestion simplement assurantielle du risque à un processus transverse et globale de création de valeur pour l'entreprise (la gestion globale du risque).

Toutefois, l'un des points clés à relever est le fait que la gestion des risques soit en constante évolution. Les méthodes s'enrichissent et la fonction de Risk Manager se renforce, se spécialise.

Dans cet enjeu de nécessaire évolution. La proposition d'une « prospective du risque » trouve tout son sens afin d'éclairer la manière de gérer les risques.

Repousser l'horizon de temps pertinent dans la prise en compte des risques, penser aux temps longs, penser l'impensable, chasser les idées reçues pour mieux éviter et/ou gérer les crises complexes et non conventionnelles, appréhender le risque dès l'innovation, repérer les signaux faibles… ;telles sont les lignes de conduite d'une «prospective du risque». Cette dimension s'appréhende alors tant au travers des outils (cartographie des risques, méthode des scénarios, arbres des causes, arbre des défaillances…) et méthodes (MADS-MOSAR) que de la vision de la gestion prospective des risques, selon Sean Cleary, (2010, p43).

Notre thème de recherche est « La mise en place d'une démarche prospective de gestion des risques au sien de la Direction Informatique de la Direction Générale du Budget».

❖ Problématique :

Dans ce cadre notre problématique se présente comme suit : « ***est-ce-que la méthode MADS-MOSAR peut aider les gestionnaires pour assurer une meilleure gestion prospective des risques informatiques au sein de la direction informatique de la direction générale du budget?*** ».

Cette interrogation principale nous conduit à ces sous questionnements :

- qu'est-ce qu'un risque informatique ?
- qu'est-ce une gestion prospective des risques ?
- comment peut-on appliqué la méthode MADS-MOSAR dans la gestion des risques au sien de la DI de la DGB ?

L'hypothèse :

« L'hypothèse peut être envisagé comme une réponse anticipée que le chercheur formule à sa question spécifique de recherche. Mannheim et Rich la décrivent comme un énoncé déclaratif précisant une relation anticipée et plausible en entre des phénomènes observés imaginés » selon Gordon. M et Petry. F (2000 : p41).

« Une hypothèse est une proposition qui anticipe une relation entre deux termes qui, selon le cas, peuvent être des concepts ou des phénomènes. Une hypothèse est donc une proposition provisoire, une présomption, qui demande à être vérifiée » selon Raymond Quivy ET Lac Van (1995 : p135).

Afin de répondre à la question principale de notre problématique, nous avons choisi l'hypothèse suivante :

La méthode de MADS-MOSAR peut être une approche efficace afin d'assurer une meilleure gestion prospective de risque au sien de Direction Informatique de la Direction Générale du Budget.

Le terrain d'étude :

Parmi les directions de la Direction Générale du Budget nous citons la Direction Informatique(DI), lieu de l'élaboration de notre travail de recherche. Cette dernière est placée sous l'autorité d'un directeur et dépend directement au directeur général de la DGB du Ministère des Finances Algérien. Selon le Décrit exécutif n° 07-364 de la 28/11/2007.

Pour mieux présenter les informations obtenues à travers notre étude, nous avons jugé nécessaire de diviser notre travail de recherche en trois chapitres :

- Le premier chapitre qui se dévisse en deux sections. La première est consacrée à la revue de littérature. La deuxième section pour le cadre conceptuel de la recherche, qui lui-même est dévisse en deux sous-section. Première sous-section trait le lien entre la gestion des risques et le système informatique, et pour la deuxième sous-section en va voir l'implémentation de la prospective en gestion des risques.
- Le deuxième chapitre se compose de deux sections. Le cadre méthodologique en première section et la présentation de l'organisme d'accueil en deuxième section.
- Le troisième chapitre consacré à l'analyse des résultats à l'aide de la méthode MADS-MOSAR. Ici on a donné une analyse on applique la méthode MADS-MOSAR au sein de la direction informatique de la DGB.

Finalement, on peut dire que ce modeste travail reste une étape importante dans la recherche scientifique qui concerne la démarche de gestion prospective des risques informatiques au sein des établissements publics algériens. Cela ouvre les portes devant nous et tous les chercheurs pour réaliser des recherches profondes dont le but de comprendre les changements stratégiques dans le monde de la gestion prospective des risques.

CHAPITRE I : REVUE DE LITTERATURE ET CADRE CONCEPTUEL DE LA RECHERCHE

Dans ce chapitre, nous avons découpé ce chapitre en deux (02) sections à savoir la revue littérature d'une part et, d'autre part, le cadre conceptuel que lui-même et dévissé en sous-section. La première sois section c'est la gestion des risques liés au système d'information et la deuxième l'implémentation de la prospective stratégique en gestion des risques.

Section n°01 : La revue littérature

Cette partie de notre travail consistera à passer en revue les principales recherches qui ont été effectuées sur la méthode MADS-MOSAR dans le domaine de l'analyse des risques.

La méthodologie d'analyse des dysfonctionnements des systèmes (MADS) est le résultat des travaux et des réflexions menées depuis 1980 par un certain nombre d'enseignants / chercheurs de l'IUT HSE de Bordeaux et d'ingénieurs du CEA.

Le groupe MADS, ainsi constitué, va axer ses efforts dans l'émergence et la consolidation d'une science du danger au terme de réflexions sur une problématique commune d'appréhension des dangers, d'une part, avec l'ambition de créer un pôle commun d'analyse et de compréhension des dangers, des risques et de leur prévention, dans des disciplines aussi variées que l'ergonomie, l'hygiène et la sécurité industrielles, la fiabilité humaine, la sécurité des installations, la sûreté des entreprises, le génie sanitaire, l'écologie appliquée, l'épidémiologie, la toxicologie et l'écotoxicologie, la gestion des crises, etc. d'autre part.

Le groupe MADS va :

- Définir la Science du Danger comme le corps de connaissances qui a pour objet d'appréhender des Événements Non Souhaités.
- Adopter un modèle systémique de référence qu'il nomme " processus de danger ".

Ce processus de danger se construit en plusieurs phases :

- La première consiste à établir une représentation générale des systèmes source et cible.
- La deuxième consiste à établir une représentation des processus sources de dangers et des processus susceptibles de subir l'effet du danger.
- La troisième consiste à modéliser le processus de danger.

Quatre types de systèmes sont retenus comme sources ou cibles de danger : l'individu isolé (acteur), la population (réseau d'acteurs), l'écosystème (environnement) et l'installation / entreprise (éco-socio-système).

Selon le groupe MADS, les relations bijectives entre chacun des quatre systèmes conduisent à proposer des points de vue sur l'une ou l'autre des multiples disciplines qui

abordent les questions de risques, de dangers, de santé et sécurité, de conditions de travail, de risques majeurs, selon OLIVIER GRANDAMAS5 (2012).

La méthode MOSAR est proposée par Pierre PERILHON (Ingénieur à (ENSAM), Ancien responsable de sécurité-sûreté au(CEA). Elle s'appuie sur la méthodologie d'analyse des dysfonctionnements des systèmes (MADS). Cette méthode offre des outils pour analyser et neutraliser les risques techniques dans les installations humaines, aussi bien au stade de leur conception que sur des installations existantes (diagnostic) selon PIERRE PERILHON (2012).

La méthode MOSAR s'articule autour d'une vision macroscopique des risques et une vision microscopique des risques.

La vision macroscopique (premier module de la méthode) consiste à réaliser une analyse des risques principaux. L'installation est modélisée. Autrement dit, elle est découpée en systèmes de proximité potentiellement sources de danger, les sources de dangers sont identifiées, puis les scénarios d'accidents sont envisagés et hiérarchisés, des objectifs sont définis et les moyens de prévention pour les atteindre sont arrêtés. L'acceptabilité des risques est négociée avec les acteurs du système, par exemple, au moyen d'une grille probabilité/gravité selon MUNOZ.F, PERRIN.L, SARDIN.M, JOSIEN.J.P, (2006).

Durant ces années 90, le groupe MADS travaille sur le vocabulaire du Danger et son homogénéisation dans la méthode MOSAR. Imprégnée de la problématique systémique et du vocabulaire défini en commun, elle devient MADS-MOSAR. Depuis les années 85, quelques étudiants l'ont utilisée lors de leur stage mais aussi en projet tuteuré en collaboration avec des entreprises où la méthode MADS-MOSAR constituait le socle de l'analyse des risques dans les installations industrielles. Le premier projet d'envergure mené par le Département HSE et l'usine SAFT de Bordeaux a permis de conduire une analyse qui a abouti à la conception du POI. Depuis cette époque une trentaine d'étudiants en stages de fin d'année ont intégré, de façon significative, cette méthode à leurs travaux selon MUNOZ.F, PERRIN.L, SARDIN.M, JOSIEN.J.P, (2006).

Au terme de ces deux modules, tous les scénarios de dysfonctionnements doivent avoir été prévus, identifiés et les informations nécessaires à l'instruction de la prévention des risques doivent avoir été rassemblées.

Section n°02 : Le cadre conceptuel

Sous-section 01 : Gestion des risques liés au système d'information.

1. Définition de système informatique :

Pour DAYAN & al (2004 : p1075) et DEYRIEUX (2003 :p11), le système informatique est le support technique du SI et sa partie croissante. Il comprend : les technologies de l'information, les ordinateurs, les applications, les réseaux et les autres systèmes qui permettent à tous d'accéder à l'information, de l'analyser, de la créer, de l'échanger et de l'utiliser.

En allant dans le même sens, VOLLE (2004 : p11) énonce que le système informatique est « L'ensemble des moyens matériels et logiciels assurant le stockage, le traitement et le transport des données sous forme électronique ».

2. Risques informatiques :

Avant de présenter un essai de panorama de risques informatiques, il est nécessaire de comprendre au préalable ce que l'on entend par risque.

2.1. Définition du risque :

D'après le document ISO guide 73, le risque est défini comme « l'effet de l'incertitude sur l'atteinte des objectifs ». Cet effet correspond soit à un écart négatif, soit à un écart positif par rapport à l'objectif initialement fixé (CLAUDE, 2012 :p39). En général, l'écart positif correspond à une opportunité.

Par contre, pour l'IFACI (in Renard, 2010 : p155), un risque est défini comme « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise ».

Le risque informatique devrait donc être considéré comme le risque dû à l'utilisation, la possession, l'exploitation, l'influence et l'adoption de l'informatique dans une organisation.

Pour que l'on puisse parler de risque, la combinaison de deux (02) éléments est préalablement nécessaire. En effet, il faut d'une part, qu'il y'ait une menace et d'autre part, que l'on soit vulnérable à cette menace.

RISQUE = MENACE * VULNÉRABILITÉ

D'après la norme ISO/CEI 27002 : 2005, la menace est définie comme « la cause potentielle d'un incident indésirable pouvant entraîner des dommages au sein d'un système ou d'un organisme ». La vulnérabilité (encore faille ou brèche) quant à elle est définie

comme « la faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace » (CLAUDE, 2012 : p41-42). En effet, le bien dont il est question ici est en fait un actif informationnel.

2.2. Les types de risques informatiques :

Les risques informatiques peuvent être présentés selon diverses approches (fonctionnelle, par nature, synthétique, etc.). L'approche synthétique ayant l'avantage d'identifier les principaux risques informatiques est à considérer prioritairement dans l'entreprise (DARSA, 2013: p218), c'est elle que nous adopterons pour la présentation des types de risques informatiques **(Annexe I, page 83)**.

Les risques informatiques peuvent avoir divers sources ou facteurs. Selon la nature de la source du risque, nous distinguons les risques humains, environnementaux et technologiques.

2.2.1. Risques humains :

Les risques humains sont ceux causés par les hommes. BARTHELEMY (2004 : p87) dans son discours sur les atteintes sur un actif matériel affirme que : l'intrusion, la fraude et la malveillance sont les risques dont la source est une personne ayant la volonté de nuire et dont l'objet du risque est généralement un matériel (endommagement ou vols de bien). Plus précisément, il distingue :

- l'intrusion : il s'agit de l'accès des personnes non autorisées dans locaux ;
- la malveillance : il peut s'agir d'un détournement de mot de passe (un informaticien peut détourner le mot de passe d'un utilisateur à son insu afin de bénéficier de tous les privilèges qui lui sont accordés) ;
- la fraude : la fraude concerne tous les salariés de l'entreprise, seuls ou en collusion avec des complices externes à l'entreprise ;
- vols : il s'agit des détournements d'actifs informatiques ;
- endommagement : il s'agit de la destruction du matériel informatique. Il peut être volontaire (sabotage) en raison de la mauvaise foi ou involontaire (maladresse ou erreur de manipulation).

Complétons ces sources de risques avec CALE & al. (2007 : p57) qui considèrent comme risques de source humaine, les erreurs humaines (erreur de conception, erreur de programmation, erreur de configuration et erreur par négligence).

Rajoutons à cette catégorie, le social engineering (les pirates, hacker, cracker) et le phishing (technique utilisée par les pirates pour se faire passer pour un organisme connu auprès de leur victime).

2.2.2. Risques environnementaux :

Nous distinguons dans cette catégorie, l'hygrométrie, les changements brusques de température (DELEUZE, 2013 : p 299).

Les sinistres et l'électricité sont également des sources de risques dus à l'environnement. En effet, pour BARTHELEMY (2004 :p72), les sources naturelles de risque sont assez diversifiées. Il considère comme étant un sinistre, les inondations, les mouvements de terrains, les raz de marrées, les éruptions volcaniques, les tremblements de terre, les explosions pour ne citer que ceux-là. En ce qui concerne les risques dus à l'électricité, ils proviennent généralement des surtensions, des sous-tensions et des coupures de courant.

Les concepteurs de matériaux électroniques devraient prendre en compte la menace que peut constituer l'électricité mais aussi la poussière pour les matériaux informatiques lors de leurs conceptions. En général, les appareils électroniques situés à proximité de la mer se détériorent plus rapidement du fait de la brise.

2.2.3. Risques technologiques :

Ce sont les risques causés par tout ce qui est lié à l'aspect technologie de l'entreprise. Ils peuvent affecter les données, les logiciels mais aussi les informations stockées par l'entreprise. Nous distinguerons dans cette rubrique les malwares, les spams, les atteintes à la disponibilité des services.

Les malwares : Pour CALE & al. (2007 : p43), « malware » est utilisé pour désigner l'ensemble des programmes malveillants qui peuvent être utilisés par les pirates afin de commettre leurs méfaits. Les principaux malwares sont :

- le virus informatique : similaire à un virus biologique qui se fixe à l'intérieur d'une cellule, le virus informatique est un logiciel qui s'introduit dans les programmes des utilisateurs, se reproduit et contamine le plus grand nombre de leurs fichiers. Les cinq (05) catégories de virus existant sont les virus du secteur d'amorçage ou boot sector, les virus d'application, les virus furtifs, les virus flibustiers et les virus polymorphes ou mutants ;
- vers informatique : contrairement au virus, un vers est un programme autonome qui n'utilise pas de support (vecteur) pour se propager car il se déplace dans les réseaux informatiques grâce à sa capacité de duplication ;

- cheval de Troie : c'est un logiciel qui se présente sous une forme bénigne en apparence (jeux, utilitaire, etc.) mais qui recèle en lui un grand péril pour l'utilisateur qui l'installera sur ma machine. Dès lors que l'utilisateur se servira du logiciel, le logiciel effectuera avec toute la discrétion possible des vols ou destructions de données par exemple et ceci à l'insu de l'utilisateur du logiciel. Il est généralement employé dans les cas de chantage, d'espionnage commercial/industriel, détournement de fond, et de prise de contrôle à distance, relais spam etc. La bombe logique est un type particulier du cheval de Troie qui s'active à un moment précis et cause par la suite un maximum de dégâts (formatage du disque dur, corruptions des données, etc.) au sein du système dans lequel il a réussi à s'introduire ;
- back door : il s'agit d'une fonctionnalité insérée dans un logiciel ou système d'exploitation par un développeur ou autre logiciel dans le but d'accéder à certaines fonctions sans devoir s'authentifier au préalable ;
- logiciels espions : il s'agit des logiciels utilisés pour voler des données. On distingue les spywares (petits logiciels s'installant à l'insu des utilisateurs), les key logger (petit programme qui enregistre secrètement les informations tapées au clavier des ordinateurs par les utilisateurs) et l'adware (collecteur d'informations personnelles pour transmettre aux sociétés faisant le marketing en ligne) selon CALE & al. (2007 : p44).

Les spams :

Le spam ou pourriel désigne l'envoi massif de courriers publicitaires dans les boîtes aux lettres électroniques des personnes sans leurs approbations d'après CALE & al. (2007 : p55).

Les atteintes à la disponibilité des services (déni de service) :

Le déni de service est un type d'attaque ayant pour but de rendre indisponible un service ou bien d'en détériorer la qualité afin de l'empêcher de répondre aux demandes légitimes d'après CALE & al. (2007: p66).

3. Gestion des risques informatiques :

Afin de mieux cerner cette partie, il convient de présenter au préalable ce que l'on entend par gestion des risques.

3.1. Définition de la gestion des risques :

La gestion des risques est définie comme un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque société qui permet aux

dirigeants de maintenir les risques à un niveau acceptable pour la société. Cette gestion poursuit principalement quatre (04) objectifs :

- créer et préserver la valeur, les actifs de l'organisation ;
- sécuriser la prise de décision et les processus de l'organisation pour favoriser l'atteinte des objectifs ;
- favoriser la cohérence des actions avec les valeurs de l'organisation ;
- mobiliser les collaborateurs de l'organisation autour d'une vision commune des principaux risques et les sensibiliser aux risques inhérents.

Toutefois, l'efficacité de tout dispositif nécessite au préalable la définition d'une bonne politique de gestion des risques car c'est elle qui donne l'impulsion à cette activité et définit les responsabilités des principaux acteurs.

3.2. La politique de gestion des risques informatiques :

La politique de gestion des risques informatiques est généralement incluse dans la politique de sécurité informatique. Il s'agit d'un document qui présente les buts et les orientations du management.

Une politique de sécurité informatique contient quatre (04) thématiques clés que sont :

- la gestion des risques fondée sur l'évaluation et la réduction des risques ;
- la qualification de l'information fondée sur une classification de l'information destinée à adapter le niveau de protection de celle-ci ;
- la conformité des systèmes avec les politiques et standards de sécurité en vigueur ;
- la sensibilisation à la politique de sécurité SI fondée sur une communication adéquate auprès de chaque employé (en modes « push et pull ») selon le CIGREF (2009 : p120).

La politique de gestion des risques informatiques formule les objectifs du dispositif de gestion des risques en cohérence avec la culture de l'organisation, le langage commun utilisé, la démarche d'identification, d'analyse et de traitement des risques et le cas échéant, le seuil de tolérance (HERVE, 2014 :p06).

3.3. Les stratégies de mitigation des risques informatiques :

Les risques informatiques peuvent avoir d'importantes répercussions sur la réalisation, le bon fonctionnement de l'organisation. Une fois le risque identifié, il convient de choisir la position ou l'option face à ce risque. En effet, il s'agit des différentes parades ou postures qu'il est possible d'adopter vis-à-vis du risque par rapport au seuil de tolérance.

- L'atténuation (mitigation) des risques est une méthode systématique utilisée par la haute acceptation du risque : il consiste à accepter le risque potentiel et de continuer l'exploitation du système informatique ;
- évitement : il s'agit d'éviter le risque informatique en éliminant la cause et/ou la conséquence des risques (par exemple, renoncer à certaines fonctions du système ou arrêter le système lorsque les risques sont identifiés) ;
- mitigation du risque : il s'agit de limiter le risque par la mise en œuvre des contrôles qui minimiseront l'impact négatif d'une menace et l'exercice d'une vulnérabilité (par exemple, l'utilisation de soutien, de prévention, de contrôle de détection). Dans certains cas, il s'agira simplement de mettre en œuvre des contrôles pour réduire le risque à un niveau acceptable ;
- transfert de risque : il consiste à transférer le risque en utilisant d'autres options pour compenser la perte, tels que l'achat d'assurance, la sous-traitance. Dans la pratique, on observe souvent chez certaines entreprises que pour atténuer le risque de perte de données, elles préfèrent faire appel aux sociétés spécialisées dans le stockage des données. D'autres sociétés font parfois appel aux structures spécialisées dans la production de service internet afin de limiter le risque d'indisponibilité de connexion internet selon NIST (2002 :p 27).

Direction pour réduire le risque. L'atténuation des risques peut être atteinte par l'une des options suivantes :

Une fois l'option choisie, le gestionnaire du risque informatique procède à son application en gardant de vue le niveau de risque fixé par l'entreprise. Généralement, la mise en application de l'option choisie est suivie de monitoring (contrôle et suivi des contrôles) de la part des instances de contrôle. La présentation des principaux risques informatiques et leurs différentes stratégies de mitigation ayant été faite, présentons les principaux référentiels qui gouvernent cette gestion des risques liés au SI.

3.4. Aperçu des méthodes de gestion des risques liés au système d'informatique :

Les instances professionnelles CLUSIF, AMRAE, APSAD ont développé depuis plusieurs années des méthodes de gestion des risques (reposant sur l'analyse de scénario de type « conséquences-causes-origines » et qui ont pour but de permettre une planification des besoins et des actions de sécurité. Le tableau ci-dessous présente les différentes méthodes qu'on peut avoir :

Tableau 1:Différentes méthodes de gestion des risques informatiques

Méthode de type « Analyse des risques»	**Méthode de type « Approche par les processus»**
MEHARI MADS-MOSAR EBIOS	Approche du DSIS Approche de COBIT Norme BS7799

Source : DESROCHES & al. (2007 :p 209).

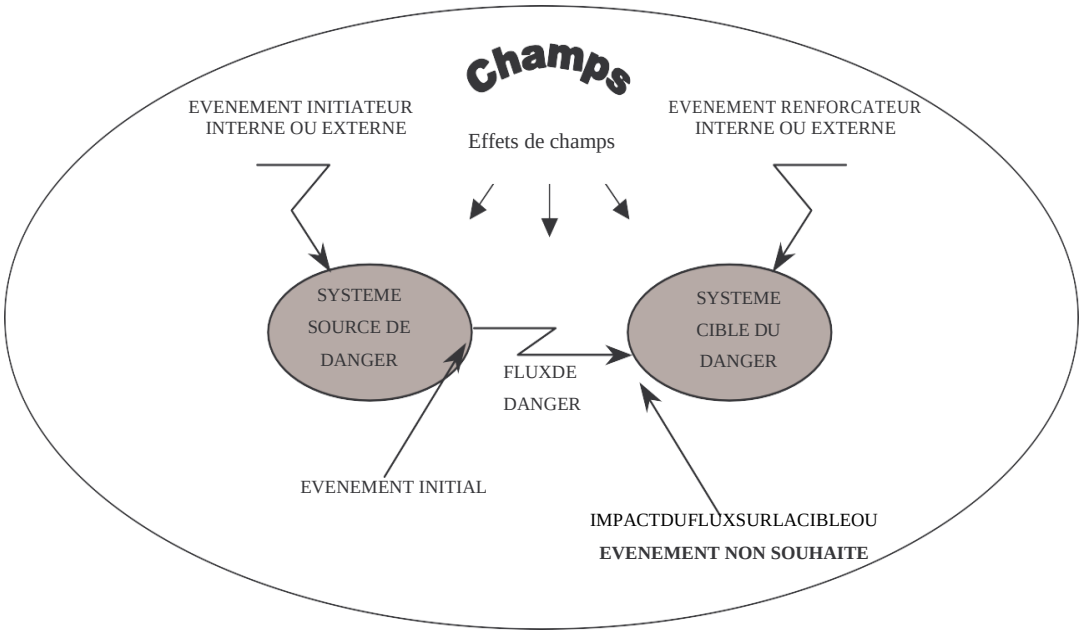
Dans le cadre de ce travail, nous ne présenterons que l'outil que nous allons utiliser à savoir MADS-MOSAR.

3.4.1. La méthode MADS-MOSAR :

MOSAR (Méthode Organisée et Systémique d'Analyse des Risques), une méthode d'analyse des risques reposant sur un modèle d'accident proche de celui de Domaine et formalisant un grand nombre des étapes de l'analyse des risques. C'est une méthode nécessitant la réflexion d'un groupe de travail concerné par le système étudié. Ce travail de groupe est aussi souvent implicitement préconisé dans la plupart des méthodes précitées.

Le modèle d'accident nommé MADS (Modèle d'Analyse des Dysfonctionnements des Systèmes) définit l'accident comme un événement non souhaité résultat de l'atteinte d'une ou plusieurs cibles du danger par un flux de danger lui-même issu d'une source de danger.

Figure 1: Le modèle d'accident selon P. Périlhon : MADS [PERILHON 2000]



Source : Livre gestion des risques de P. Perilhon 2000

Ce modèle repose sur les notions :

- de système(s) source : système(s) à l'origine des flux de danger donc des événements non souhaités.
- de système(s) cible : système(s) sensible(s) aux flux de danger et subissant des dommages.

Il existe quatre types de cibles déjà citées.

- d'événement initial : événement qui caractérise le changement d'un système qui passe d'un état ou d'une situation normale à un état ou une situation défaillante.
- d'événement non souhaité : ensemble de dysfonctionnements susceptibles de provoquer des effets non souhaités sur des systèmes cibles.
- de flux de danger : vecteur du danger déclenché par l'événement initiateur.
- d'événement initiateur qui va déclencher l'événement initial.
- d'événement renforçateur qui accroît la vulnérabilité de la cible ou augmente les effets.

Cette méthode a priori, développée au CEA intègre l'approche déterministe du risque et l'approche probabiliste lorsque cela est possible. On peut considérer un grand nombre de types d'accident puisque l'on applique ce modèle d'accident (basé sur le processus de danger) sur le ou les champs d'application qui nous intéressent. On aboutit à la construction de scénarios dans lesquels on peut ensuite mettre en place des mesures de prévention ou de protection en les définissant précisément dans la durée et dans leur action sur le système.

Les étapes principales de la méthode sont caractérisées par:

- un module de définition du système s'appuyant sur les principes de la systémique [LE MOIGNE 1977]. On considère alors le système à étudier, son environnement extérieur et ses interactions avec les autres systèmes. Si le système est trop important, on le décompose alors rigoureusement en sous-systèmes ayant les mêmes propriétés.

- un module d'identification des risques qui passe par l'identification des sources et des cibles du danger. On peut utiliser les arbres logiques pour représenter les processus d'accident (cf. l'AMDE).
- un module d'évaluation des risques qui utilise la même grille gravité / probabilité que l'AMDEC à laquelle on associe la limite d'acceptabilité de Farmer permettant de distinguer les risques acceptables des risques inacceptables. Les risques inacceptables feront alors l'objet d'actions prioritaires de prévention.

- un module de proposition de solutions pour rendre les risques inacceptables acceptables. On sort alors du domaine de l'audit. On définit (et caractérise) ensuite les solutions choisies (quoi, par qui, comment, fréquence des vérifications,…).
- un module de vérification de l'efficacité et donc de validation des solutions choisies.

4. Les acteurs de la gestion des risques informatiques :

Les principaux acteurs de la gestion des risques informatiques sont : la Direction Générale, le Risk Manager, le RSSI.

4.1 La Direction Générale :

Selon GREUNING & al. (2004 : p33), il est de la responsabilité de l'équipe dirigeante, et de la Direction Exécutive de définir les orientations stratégiques et de les suivre en ce qui concerne la gestion des risques au sein de l'organisation.

En effet, la Direction Générale fait partager à toute l'entreprise la vision d'une gestion rigoureuse et efficace du risque, donne l'impulsion de celle-ci et crée les conditions de mise en œuvre du processus de management des risques. Il est également de sa responsabilité d'instaurer une bonne culture de gestion des risques au sein de l'entreprise sur le giron de la gouvernance des risques avec pour objectif principal, la maîtrise des risques.

4.2. Le Risk Manager (RM) :

Selon le CLUSIF- AMRAE (2006 :p04), le RM est chargé de concevoir les méthodes et les outils de gestion des risques (cartographie des risques, etc.), d'élaborer et de mettre en œuvre la politique et le plan d'assurance de l'entreprise, de conseiller les métiers sur les mesures de prévention, de protection, de détection et de réaction face au risque.

4.3. Le RSSI :

Le RSSI (responsable de la sécurité des systèmes d'information) est chargé de prévenir les risques dès leur phase de développement, de proposer des plans d'action de réduction et de contrôle des risques, de suivre la mise en place des actions décidées, de rendre compte à la Direction Générale et de communiquer sur la sécurité du SI avec le ou les Directeurs en charge des SI (CLUSIF-AMRAE, 2006 : p04).

Sous-section 02 : L'implémentation de la prospective stratégique en gestion des risques.

1. La prospection stratégique :

Le terme de prospective nous vient du latin prospicere (regarder au loin, de loin, discerner quelque chose devant soi). Comme le rappelle Michel Godet (2007 : p11), « l'attitude prospective est née d'une révolte de l'esprit contre le joug du déterminisme et le jeu du hasard ». Elle consiste en une approche du futur visant l'anti fatalité (Hugues de Jouvenel) et l'antihasard (Pierre Massé).

Pour Gaston Berger (1959), la prospective doit permettre de « voir loin, large, profond, penser à l'homme, prendre des risques ». À cela s'ajoute le fait de voir autrement (se méfier des idées reçues), de voir ensemble (réflexion fondée sur le groupe et visant l'appropriation par l'ensemble des parties prenantes sauf dans une dimension stratégique confidentielle où cela est limité à un groupe plus restreint) et d'utiliser des outils et méthodes pour la rigueur de la démarche prospective.

La prospective est souvent présentée comme une « indiscipline intellectuelle », à savoir une vision englobant regardant chaque problème au niveau local tout en traitant l'ensemble des questions à un échelon global.

La prospective comprend également une dimension humaine et organisationnelle en répondant aux difficultés des organisations. Elle aide à penser la conduite du changement. Elle vise l'appropriation par le groupe, ce qui suppose une réflexion collective. (Groupe restreint ou élargi selon les objectifs concernés).

Sa dimension est encore stratégique, de nombreux usages ont été faits de la prospective en matière économique, pour des ministères, des entreprises et des territoires (collectivités).

« Pas de prospective sans rétrospective » nous dit encore Michel Godet. La prospective vise à regarder l'héritage accumulé, l'état de l'art dans le domaine étudié afin de mieux prendre en compte les tendances lourdes, les germes de changement, les incertitudes clés ou les ruptures critiques, de repérer les fausses innovations et de mieux cerner ce qui est du domaine du vrai et du domaine des idées reçues. Elle permet de soulever le doute face à une vérité, se méfier des consensus et des prénotions du sens commun, car in fine la seule certitude réside dans l'existence d'incertitudes.

La prospective s'articule autour d'une relation triangulaire, appelée triangle grec : L'anticipation permet l'action par l'appropriation. Telles sont les trois composantes du

triangle grec de la prospective imaginé en 1984. Ainsi, la prospective ne se résume pas à l'anticipation seule, elle consiste en un processus visant la réflexion par les parties prenantes de la démarche de prospective (notamment dans le cadre d'ateliers de prospective). Cette réflexion aura comme sous-jacent une démarche d'anticipation ainsi que d'études des différents futurs possibles afin de mieux préparer l'action future.

1.1. Le triangle grec de la prospective: **(Annexe II, page 86)**

1.1.1. L'anticipation :

« L'avenir ne s'attend pas, il se prépare » nous dit Sénèque. « Il ne se prévoit pas, il se prépare » nous dit encore Maurice Blondel. L'avenir ne peut être attendu passivement et la réactivité n'est pas satisfaisante dans la mesure où l'urgence rime avec l'insuffisance (dans la prise en compte du futur). « Quand c'est urgent, il est trop tard » (Michel Godet). L'avenir reste à écrire, pouvoir le prédire avec exactitude est synonyme d'imposture. D'où la nécessaire anticipation du futur, dimension première du triangle grec et caractérisant la démarche prospective. Elle consiste à avoir une vision de l'environnement passé, présent et futur. Il s'agit encore de dégager les incertitudes majeures, les tendances probables, les évènements à survenance vraisemblable, les points sujets à controverse. Elle se base sur un diagnostic précis, une analyse chiffrée afin d'éclairer l'avenir par des outils précis et une démarche rigoureuse.

1.1.2. L'appropriation :

Il est ici question d'une démarche de réflexion collective, l'appropriation par le groupe permet l'anticipation favorable à l'action. Cette composante est donc centrale dans la démarche prospective. Une appréhension par les différentes parties prenantes de l'organisation permet ainsi de favoriser une démarche d'organisation apprenante[21]. Il s'agit ici de favoriser la motivation de chaque partie prenante et de développer une mobilisation collective afin de créer des synergies et éviter les inerties. « Elle constitue un point de passage obligé pour que l'anticipation se cristallise en action » nous dit Michel Godet. Pour mener à bien une action et que des projets ne restent pas lettres mortes, il est indispensable que ceux qui les mènent à bien se sentent concernés et soient impliqués.

1.1.3. L'action :

Anticiper le risque et y réfléchir collectivement constitue le socle de base d'une bonne préparation des actions à mettre en œuvre au sein des entreprises et des territoires. Une fois les deux étapes précitées amorcées, l'action en est la suite logique, celle-ci est donc d'autant plus efficace et pertinente qu'elle a été préparée collectivement et qu'elle se veut

anticipatrice. Il est alors question de se préparer aux changements attendus (pré activité) et de provoquer les changements souhaités (pro activité, concernant les objectifs stratégiques).

En répondant à ces trois composantes du triangle grec, la prospective permet de « ne pas s'écarter des futurs possibles avant d'être certain que l'on a plus rien à apprendre d'eux » pour reprendre Richard Bach.

Tel est l'un des objectifs de la prospective, appréhender les différents futurs possibles (futuribles) et tenter de tirer des leçons sur et pour l'avenir de cette pluralité de schémas de situations potentiellement réalisables.

La prospective répond ainsi à la question « que peut-il advenir ? » (Une question préalable vise à se demander « qui suis-je ? », une connaissance préalable de l'organisation est un point important, le connais-toi toi-même de la philosophie antique).

Dans sa dimension stratégique, elle vise à se demander « que puis-je faire ? »

Se posent également les questions du « que vais-je faire ? » et du « comment le faire ? » La réponse à ces questions permet de mieux cerner l'avenir et de tenter d'apprendre du futur, de se représenter quels sont les futurs probables et vraisemblables. L'avenir reste ouvert et la détermination doit permettre d'aller au-delà des déterminismes. Le chemin étant le but, la prospective doit permettre de créer le cheminement permettant d'arriver aux buts souhaités.

2. Analyse de la dimension prospective de la gestion des risques :

Le Risk Management ayant une dimension proactive, il est question de démontrer que la gestion des risques, dans sa visée, comme dans ses méthodes répond aux trois composantes du triangle Grec précité ainsi qu'aux questions indispensables à se poser face à l'avenir.

Le cadre d'analyse proposé est donc celui des questions clés à se poser face à l'avenir tiré de la démarche prospective telle qu'appréhendée par « l'école française de prospective » (Laboratoire d'innovation, de stratégie et d'organisation du Conservatoire National des Arts et Métiers). D'autres approches (anglo-saxonnes) peuvent néanmoins être prises en compte.

2.1. La réponse du Risk Management aux questions à se poser face à l'avenir.

Dans le cadre d'une approche prospective, il existe quatre questions à se poser face à l'avenir et une question préalable à celles-ci concernant la connaissance de l'organisation.

Il convient, avant d'entrer dans le détail de préciser, et pour reprendre l'approche de Jean Le Ray (2010 : p32), qu'un système de management des risques doit, pour être utile et efficace :

- impliquer la Direction et associer l'ensemble des acteurs (intégration des parties prenantes),

- permettre d'anticiper les sinistres et pérenniser les solutions déployées (approche prospective),

- organiser les démarches et mesurer le progrès (démarche d'organisation apprenante).

2.1.1. **« Qui-suis-je ? » Le Risk Management, sources d'effets d'expériences pour les entreprises (organisations apprenantes).**

Une question préalable afin de pouvoir étudier l'avenir d'une organisation consiste à se demander si l'organisation a une connaissance suffisante d'elle –même (qui suis-je ?).

Le Risk Management permet-il de répondre à cette difficile question du connaît-toi toi-même. Question qui, dans une perspective de gestion des risques, trouve tout son sens.

Le dispositif de Risk Management, en posant les questions suivantes (quels sont les risques qui peuvent l'affecter, d'où proviennent-ils et comment l'organisation peut-elle les traiter ?), permet de mieux connaître l'organisation. Connaître l'exposition aux risques d'une organisation revient à accroître la compréhension du fonctionnement de celle-ci (c'est l'une des dimensions stratégiques du Risk Management).

Une autre question connexe sera celle qui consiste à connaître la réaction de l'organisation face à la survenance d'un risque, c'est toute la problématique de la gestion de crise, laquelle peut être préparée au mieux à l'aide de dispositif de gestion des risques.

Pour ce faire, le Risk Management s'appuie sur la connaissance acquise au travers des différentes démarches de maîtrise. Il consiste à maîtriser les obstacles s'opposant à l'atteinte des objectifs et par ce fait est au fondement du management de l'organisation. Le Risk Management, de par ses caractéristiques, est une fonction fédératrice, coordinatrice, permettant d'accroître la connaissance de l'organisation sur elle-même.

La fonction Risk Management est transverse (application d'un langage commun dans l'entreprise en termes de gestion des risques, cohérence du niveau globale d'exposition au risque selon les différentes entités du groupe, sensibiliser chaque groupe et fonction à sa responsabilité face au risque).

Une fonction à part entière dédiée la gestion des risques permet de tendre à l'exhaustivité en matière de risques.

Le Risk Manager est également un opérationnel : sa responsabilité est en cause en cas de défaillance du système de gestion des risques (négociation dans le cadre du transfert de risque, responsabilités vis-à-vis des dispositifs d'alerte, de traitement des risques, mis en place…).

2.1.2. **« Que peut-il advenir ? » Quels sont les risques susceptibles de survenir ?**

La gestion des risques permet donc de mieux appréhender les contextes endogènes et exogènes à l'organisation. Pour autant permet-elle d'appréhender ce que sera demain ?

Le risque est un danger éventuel plus ou moins prévisible, mais également une condition du succès de l'action présente et future. Gérer les risques implique donc nécessairement de se demander ce qu'il peut advenir. Pour Jacques Lautour, « le risque, est un événement aléatoire dont l'occurrence n'est pas certaine, mais qu'il faut anticiper à temps pour pouvoir le gérer ». Gérer les risques implique nécessairement d'anticiper les risques, a contrario, sans anticipation, la gestion des risques se résumera à une réponse assurantielle et au traitement ex ante du risque.

L'apport principal consiste à représenter les principaux risques et les enjeux s'y rapportant afin de procéder aux décisions les plus pertinentes.

Se demander ce qu'il peut advenir : La prise en compte des trois caractéristiques du risque.

- la probabilité d'occurrence (probabilité de survenance d'un risque).

- la détectabilité des risques (dépend de la qualité de l'organisation à détecter les risques, le Risk Management peut renforcer cette capacité).

- la sévérité (se demander quel sera le coût probable en cas de survenance, coût immédiat et pertes à terme : pertes d'opportunité, impossibilité d'activité pour l'organisation, paralysie, perte d'exploitation.

2.1.3. **Dimension stratégique, la gestion des risques vise à se demander «que puis-je faire**

« Prendre des risques, ce n'est pas prendre n'importe quel risque ». (P. La gadec) Gérer les risques consiste ainsi à se demander quels risques l'entreprise va prendre, et quels sont ceux pour auxquels elle est déjà exposée.

Le Risk Management consiste à faire en sorte que les actions nécessaires face au risque soient suivies des faits.

Gérer le risque, c'est le cerner : L. Bernstein définit le Risk Management par le fait de « maximiser l'espace dans lequel nous contrôlons le résultat, tout en minimisant ceux dans lesquels nous n'avons absolument aucun contrôle…et où le lien entre l'effet et la cause nous demeure caché ».

Le Risk Management revient donc à réduire les zones d'incertitudes et à renforcer les zones de risques maîtrisés.

C'est du moins l'objectif poursuivi de gestion des risques. Face au risque, il est possible de réduire l'incertitude (sans la réduire à zéro toutefois) et de mettre les risques sous contrôle (tout système de contrôle ayant là encore ses limites).

Gérer le risque, c'est l'accepter : La gestion des risques consiste à accepter le risque et à vouloir y apporter une réponse. Tout en étant prudent face à ce dernier, il ne s'agit pas pour autant de se prémunir par la précaution (on n'accepte plus le risque, ce qui revient souvent à limiter, dans la pratique, l'action). Les dispositifs de Risk Management viseront, une fois les phases d'identification et d'évaluation faites, à déterminer quelle part de risque sera transférée (assurance, mécanismes de couverture) et quelle part de risque sera finalement acceptée et assumée par l'organisation.

La gestion du risque vise ainsi à accepter une part de risque. Il n'est en effet pas question de se focaliser sur les risques assurables uniquement, mais à aller au-delà dans l'étude des possibles. Tous les risques ne sont pas assurables (traditionnellement : perte d'exploitation, incendie, bris de machines…), mais les risques inassurables doivent quand même être pris en compte (risque d'image, risque technologique encore trop peu connu pour être assuré, risque de la chaîne logistique…).

Cela permet ainsi de « faire chanter les statistiques », de regarder la réalité autrement. Face à la diversité des solutions à risques étudiées : le Risk Management permet de présenter un large panel de solutions.

Là où les assureurs pilotent le risque en regardant dans le rétroviseur, la gestion des risques se tourne davantage vers les risques nouveaux : ceux pour lesquels la connaissance n'est pas complètent et une activité donnée est empreinte d'incertitude.

Gérer le risque, c'est l'amoindrir : il est alors question soit de le diminuer dans ses probabilités d'occurrence (prévention) ou dans son impact (protection), comme il a été vu préalablement. Dans cette optique le risque est transformé en risque moindre.

Le risque peut encore être supprimé (transformé en risque nul).

Gérer le risque, c'est le convertir en création de valeur (conversion en risque positif, création d'opportunités): l'apport du Risk Management est d'éclairer le preneur de risque sur les conséquences de son action en lui permettant de comprendre et d'identifier les sources de risques.

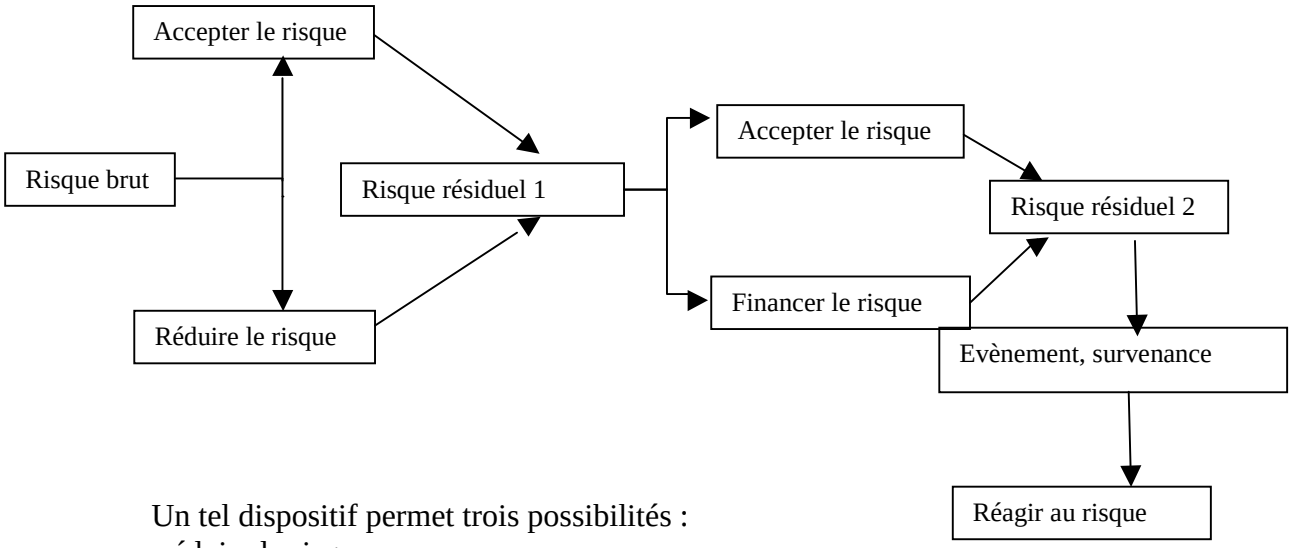
Une fois cette compréhension acquise, le risque peut être transformé d'une menace, un danger, en une opportunité : un risque à prendre, car ce dernier est maîtrisé. (Cela est d'autant plus vrai pour des risques stratégiques tels que le positionnement sur un nouveau segment, sur un nouveau marché…pour des risques plus traditionnels tels que le risque incendie, l'approche est avant tout la sécurité de l'activité).

Faire de la gestion des risques un système de management de l'entreprise : Pour Jean Le Ray (2010 : p 35), faire de la gestion des risques un système de management à part entière dans l'entreprise peut permettre de manager les risques et opportunités grâce à des processus dédiés.

Que faire face au risque ? (Source Jean Le Ray, Gérer les risques)

Le présent schéma résume les actions à mener face au risque. Un tel dispositif de Risk Management permet ainsi de formaliser une approche des actions à mener en gestion des risques.

Figure 2 : Processus général de traitement des risques.



Un tel dispositif permet trois possibilités :
-réduire le risque,
-le financer,
-réagir à l'accident.

3. Approches similaires : la «perspective gestionnaire de risque», une dimension prospective :

Gérer les risques, c'est vouloir réduire l'incertitude. Seulement cela implique donc, tout en se remémorant le passé et en pensant au présent (mode d'action courant de l'organisation), de penser à l'avenir. La « perspective gestionnaire de risque » (Yvon Pesqueux), c'est avant tout inscrire son action dans un cadre temporel. La dynamique gestionnaire revient bien souvent à penser « court terme », le présent étant le mode de pensée sous-jacent à toute action. Penser aux risques inhérents à son activité : c'est donc imaginer les conséquences non seulement à court terme, mais également dans le temps (notion d'irréversibilité des actions prises, responsabilité sociale de l'entreprise…).

La question de la gestion des risques, c'est celle du rapport de l'Homme à son environnement : celui de l'organisation, les risques endogènes à cette dernière, et l'environnement général (économie, société : risques exogènes).

Une telle dimension est à retrouver dans la démarche prospective dont l'un des objectifs est de se demander ce que sera demain, ce que comportera l'avenir.

On le voit donc, sur cette question Risk Management et Prospective sont deux approches visant à regarder dans la même direction : celle de l'anticipation.

3.1. La vigilance, trait commun entre Prospective et Risk Management.

Comme l'évoque F. Château raynaud (2003 : p53), la gestion des risques débouche sur les processus d'alerte et de vigilance. De tels concepts sont également à retrouver dans l'approche prospective: être vigilant face à l'avenir (voir loin, large, profond : la prospective est donc une vigie) et alerter sur les évènements pouvant survenir.

Nombre d'organisations pratiquant le Risk Management mettent en place ce système «de vigie ». En effet, à l'instar de l'Urssaf-IDF, une revue des risques peut être effectuée tous les trimestres afin de faire le point sur l'évolution des risques identifiés en termes de vraisemblance. La cartographie des risques se veut également évolutive, afin de coïncider avec l'évolution de l'exposition aux risques de l'organisation. « Il ne suffit pas de s'arrêter à la construction d'une cartographie des risques, il faut encore la faire vivre afin de repositionner l'entreprise dans son environnement », par nature évolutif, précise Enriqué Muro (2009 : p26).

3.2. L'anticipation est au cœur de la fonction de Risk Management.

En cherchant à prendre du recul dans l'analyse des risques afin de pouvoir identifier les probables et avoir le niveau de risque associé à chaque probable, la gestion des risques comprend une dimension anticipation.

Mieux se préparer aux menaces par l'anticipation est la quête permanente du Risk Management pour l'amélioration de la prise en compte du risque, ce afin d'éviter l'irréversibilité et de permettre la résilience (capacité de l'organisation à surmonter une crise, un évènement).

L'anticipation dans la gestion des risques c'est aussi être vigilant face aux décisions prises par l'organisation. La flexibilité et la résilience sont des concepts que le Risk Manager se doit d'intégrer afin de toujours se tourner vers l'avenir et d'anticiper au mieux les risques pouvant survenir. Il est donc nécessaire pour gérer les risques d'anticiper la gravité et l'amplitude de ces derniers afin d'imaginer des processus de traitement des risques les plus efficaces possible, mais également des dispositifs de gestion de crise adaptés à chaque situation potentiellement réalisable (Plan de continuité d'activité, cellule de crise…). L'anticipation dans la gestion des risques sera alors de renforcer la capacité à déceler les nombreux risques d'une organisation et à y apporter les réponses adéquates avant même leur survenance tout en transférant une part de ces derniers (la réactivité doit également être de mise, celle-ci étant fonction de l'anticipation faite des différents risques). Une autre notion à prendre en compte est celle de vicariance (capacité à remplacer un processus par un autre) : celle-ci sera d'autant plus efficace que les différents risques susceptibles d'affecter l'organisation auront été anticipés avec des degrés suffisamment précis.

Comme l'exprime Jacques Charbonnier (2007 : p33), « l'esprit du Risk Management consiste avant tout à se poser la question et si… ? », ce qui suppose un certain recours à l'imagination.

Il s'agira alors d'avoir recours à des méthodes telles que la méthode des scénarios trouve également à s'appliquer pour imaginer des risques encore mal connus. Une utilisation pertinente peut alors en être faite en matière de risque pays, afin de cerner l'état politique, économique et social de nations étrangères selon J. Charbonnier, (2007 : p 37).

3.3. La cartographie des risques : la représentation des futurs possibles.

La réalisation d'une cartographie des risques **(Annexe III, page 88)** est un processus de réflexion commune permettant de diagnostiquer les vulnérabilités de l'entreprise et de se représenter, pour chaque classe de risque, l'étendue des futurs possibles identifiés comme ayant un potentiel vraisemblable de survenance.

Établir une cartographie des risques répond à différents objectifs : répondre à l'obligation réglementaire de communiquer sur les risques, identifier et évaluer les risques liés à la non-conformité, réduire les risques opérationnels (sécurité, informatique…), élaborer le plan d'audit, identifier et piloter les couples risques/opportunités ou encore hiérarchiser les

risques recensés dans le cadre de l'élaboration de ladite cartographie, et in fine décider des mesures prioritaires (optimisation des ressources, définition du niveau raisonnable de prise de risque).

En répondant à de tels objectifs, la cartographie permet ainsi d'étudier les futurs possibles de l'organisation en termes de risques.

Au niveau de la méthodologie, la cartographie des risques peut être élaborée selon la double démarche top-down et Botton-up.

La cartographie des risques peut ainsi prendre différentes formes : permettre de classer les risques selon leur probabilité et leur impact (fréquence/ sévérité), selon leur nature (classe de risque), selon la part de chaque entité pour un risque (portefeuille de risques), mais également selon leur horizon (court, moyen, long terme).

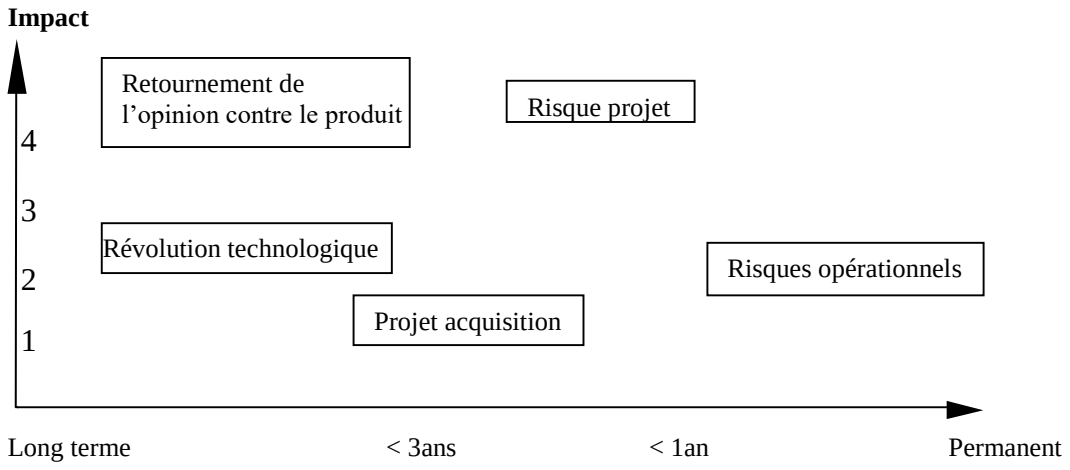
Cette dernière approche apparaît comme d'autant plus pertinente pour l'anticipation et l'identification des risques afin d'envisager un traitement proactif.

Déterminer l'horizon de temps associé à un risque est un élément clé pour s'y préparer. Les deux représentations ci-après permettent d'avoir un éclairage sur les cartographies pouvant être mises en place afin de représenter l'horizon de temps associé au risque.

Une cartographie est ainsi conçue en 2 étapes :

- l'identification des risques (voir ci-dessus, approche top-down et Botton-up) : laquelle se veut globale et détaillée
- l'évaluation du risque (probabilité, sévérité) : ce sur une base à la fois qualitative (score card, scenario) et quantitative (probabilités conditionnelles, base de données de pertes…).

Figure 3: cartographies de type « horizon des risques » : (source AMRAE)



4. Pour « une prospective du risque ». L'implémentation de la prospective stratégique en gestion des risques :

« La source de la peur est dans l'avenir, et qui est libéré de l'avenir n'a rien à craindre » M. Kundera.

Pour le Dr. Alexei Grinbaum, « notre peur et notre paralysie (à l'égard du risque) se prolongeront tant que nous n'aurons pas trouvé la bonne approche ».

Trouver la bonne approche implique de faire des propositions, (l'avenir ne s'attend pas, il se propose) l'une d'entre-elles peut consister à développer une « prospective du risque ».

Lorsqu'en 2010, il a été proposé de créer un observatoire du risque, c'est bien pour répondre à un besoin de prospective du risque, preuve de la nécessité de se projeter dans l'avenir du risque et non simplement de l'analyser dans le présent. Il est donc question, eu égard à la dimension prospective de la gestion des risques et de ses limites face à l'avenir, de proposer « une prospective du risque ».

Face aux limites évoquées de la gestion des risques quant aux risques futurs, la prospective prend alors tout son sens. « Le risque est devenu la mesure de notre action, la société du risque fait de l'avenir la question du présent » nous disait encore Ulrich Beck. Faire de l'avenir la question du présent, c'est aussi avoir ce regard prospectif, tourné vers l'avenir, dans l'action de gérer les risques.

Claude Henry (Traité des nouveaux risques) distinguait trois âges du risque : La prévoyance, la prévention et la précaution.

La prospective vient en amont : bien avant la prévention et la précaution et se substitue à la prévoyance par des méthodes claires et rigoureuses afin d'étudier les différents futurs possibles de l'avenir, ce à un horizon de temps jugé comme pertinent eu égard au système étudié.

il existe différentes approches de la prospective selon Philippe Durance, Stéphane Cordobes (2003 : p120-125). Deux approches principales peuvent être distinguées. L'approche dans le monde anglo-saxon où la futurologie y a meilleure presse, on ne parle pas de « prospective » en tant que telle mais davantage de foresight ou de strategic prospective. Ainsi avec des méthodes telles que l'horizon scanning ou encore le scenario building (très usité aux Etats -Unis), une forte culture prospective y est ancrée (au Royaume-Uni par exemple).

L'école française de prospective correspond davantage à la pérennisation des méthodes cartésiennes d'analyse des systèmes issues des travaux de la Rand Corporation.

La prospective et l'adaptation : concept flexible, la prospective peut être adaptée aux différentes organisations. La réussite d'une démarche prospective résidera notamment dans l'échange d'informations (mise en place de plate-forme d'échange, c'est tout le lien avec l'Intelligence Economique), l'utilisation pertinente du savoir présent dans l'entreprise et son intégration au processus de prospective pour le ré décliner dans l'étude des futurs possibles, ce qui facilite le retour d'expérience. Une bonne compréhension des mécanismes de l'organisation par tous à l'issue de la démarche et l'intégration d'experts dans l'entreprise afin de garantir l'existence d'un savoir-faire en la matière.

4.1. La « prospective du risque » : intérêt, apports, domaines d'application :

« Si tu n'as pas en toi assez de ressources pour tirer parti des maux qui t'arrivent, aie la prudence de les prévenir », nous enseignait Pythagore. Le diagnostic de l'entreprise (voir notamment l'analyse ressources et compétences, Hamel et Prahalad) révèle souvent un univers contraint où les moyens (humains, financiers) sont limités. Dans un tel contexte, marqué de surcroit par l'imprévisibilité, la prospective stratégique (Strategic Foresight) peut s'avérer une aide précieuse dans la prise d'action stratégique en améliorant la prise en compte des risques.

L'anticipation, l'analyse et l'interprétation des tendances lourdes du futur apparait comme de plus en plus difficile à prendre en compte.

La multiplicité des acteurs et des relations rend plus difficile que jamais la prise en compte du risque. Dans le contexte de mondialisation qu'est le nôtre, les risques pays et risques filiales sont une tendance non négligeable dont il importe de tenir compte.

L'incertitude va croissante sur les développements des risques futurs, les délais de pré - alerte ne peuvent donc être déterminés avec précision.

S'armer contre l'incertitude, voilà alors le rôle de la prospective stratégique.

Le rôle du prospectif stratégique est ainsi « d'élargir consciemment les limites des perceptions propres aux organisations pour ce qui est des défis futurs » selon leCenter for Security Studies (2009 : n°52).

Trois phases sous-tendent cette démarche : l'analyse de l'environnement et des tendances futures, la détermination des effets des différentes représentations de l'avenir obtenues (horizon scanning, scénarios), on sélectionne alors les thèmes les plus importants et les examine de manière approfondie. Vient enfin une phase visant à développer différentes alternatives d'action.

Mise en garde/ Limites :

Comme le relevait Karl Popper, une approche, aussi aboutie soit -elle, ne saurait apporter toutes les réponses, autrement elle est synonyme d'imposture, d'idéologie, de prédictions. Le critère de la scientificité réside dans son caractère contestable. Sans aller jusqu'à prétendre être une approche scientifique, la prospective permet d'apporter des éclairages sur l'avenir, un regard différent sur le futur et des outils afin de s'armer face aux incertitudes de l'avenir. Toutefois, en la matière, prétendre pouvoir prédire l'avenir avec exactitude n'est pas possible et tel n'est pas le but de la démarche prospective. Il est davantage question de se rapprocher des futurs possibles.

L'un des apports majeur de la prospective ne réside pas tant dans les rendus finaux (par exemple un rapport d'une soixantaine de pages suite à une analyse structurelle des variables clés d'un système) que dans la participation des différents membres d'une étude au processus de prospective.

Dans notre sujet, plus que les outils et méthodes développés, l'intérêt de la prospective sera de renforcer la culture du risque, la conscience des risques et la vigilance face à l'avenir de même que la confiance dans ce qui est bien appréhendé. Les outils ne sont qu'un moyen d'arriver à une fin, laquelle est de permettre de créer l'avenir en ayant une vision de ce que pourra être ce dernier.

Des pistes de réflexion prospective face aux risques :

Des pistes de réflexion de l'intérêt de la prospective face au risque sont développées ci -après. Face à la difficulté de ratisser large et loin dans le cadre du présent mémoire, les développements ci-après sont toutefois des propositions et pistes de réflexions permettant de faire le lien entre prospective et gestion des risques.

- **Les pistes d'améliorations de la gestion des risques :**
    - ✓ **Risques et prise en compte du temps dans l'action, les temps longs du risque et la prospective : repousser l'horizon pertinent en Risk Management.**

En matière d'incertitude face à l'avenir, la gestion des risques présente des limites. Pour Romain Laufer, le management des risques suppose le management des représentations du risque. Ces représentations ont leurs limites face à l'éventail des possibles en réalité. Développer une vision prospective du risque, c'est offrir une nouvelle clé de représentation des risques, laquelle vise notamment à repousser l'horizon pertinent de prise en compte du risque.

Souvent, il est difficile de distinguer clairement l'horizon pertinent en matière de stratégie, il en va de même en matière de risque. Quand bien même on ne distingue pas clairement

l'horizon, on peut tenter d'anticiper ce qui se cache derrière. Une réflexion sur les temps longs du risque est indispensable. Inscrire son action dans la durée, c'est se demander quelles seront les conséquences des choix stratégiques opérés par l'entreprise, notamment en termes de risques (par exemple de pollutions des sols, pollutions visuelles, sonores…). Comme nous l'avons vu l'actualité regorge d'exemple de risques présents depuis de nombreuses années mais se matérialisant récemment. Ainsi, concernant le cas de l'industrie pharmaceutique e et de médicaments tel que le Médiator impactant l'image d'entreprises comme le laboratoire Servier ou encore les pouvoirs publics (Afssaps…), on voit clairement les limites des dispositifs de pharmacovigilance. Souvent, les conséquences de l'usage de médicaments peuvent s'étendre au-delà d'un horizon court -terme.

L'horizon fréquemment retenu en gestion des risques se situe aux environs de trois ans. Pour avoir davantage de visibilité, l'apport de la prospective est de permettre une étude sur un horizon plus étendu, proche des 10 ans, car plus significatif face aux risques à venir et émergents (au-delà, par exemple à 15 ans, il est difficile d'avoir une visibilité). Déterminer et repousser cet horizon de prise en compte des risques peut donc permettre les décisions à court terme tout en pensant au long terme. Car bien souvent la société n'a pas de mémoire à moyen et long terme (car ce sont les hommes qui constitue la mémoire de l'entreprise), eu égard aux contraintes de l'activité à court terme.

La réussite d'une activité s'analyse dans la durée. Non seulement lors de l'introduction de l'innovation, du produit, dans la société, mais également dans la prise en compte de ses impacts futurs.

Une approche prospective des risques visent à considérer les temps longs en matière de risque. Notamment pour les risques technologiques.

Ainsi, en matière de risques liés aux déchets radioactifs, outre les défaillances éventuelles du présent qu'il convient de maîtriser, une réflexion sur le long terme s'impose. Les analyses de sûreté, même si elles sont restreintes par les connaissances du moment, doivent être tournées vers l'avenir afin d'étudier les évènements possibles. Là encore, des analyses prospectives trouvent leur pertinence. Cette réflexion a alors un sous-jacent : ne pas transmettre des risques inacceptables aux générations futures (d'où la problématique du stockage des déchets et des risques inhérents à ces derniers).

- ✓ **L'apport de la prospective pour le Risk Management, s'armer face à l'incertitude de l'avenir : quelles perceptions du risque demain ?**

L'avenir est largement empreint d'incertitude. Or, une situation d'incertitude n'est pas probabilisable, il n'existe aucune base scientifique permettant de mesurer ladite

incertitude. Une situation d'incertitude est donc un cas unique qu'il n'est pas possible d'appréhender sur la base de cas a priori similaires.

Les nouveaux risques correspondent davantage à un univers où la répétition des expériences passées fait défaut et où il est nécessaire pour le décideur de quantifier et d'évaluer la vraisemblance de scénarii.

Pour ces raisons, la prospective, en étudiant les futurs possibles peut permettre de se demander quels seront les risques à l'avenir ? Comment sera perçu le risque à un horizon déterminé ? Prendrait-on des risques de la même manière dans les 20 prochaines années ? Pour Pierre Massé, la prospective, de par sa vocation pour l'incertain, est « une indiscipline intellectuelle remettant en cause la prévision dangereuse à base d'extrapolation » (Massé, 1973).

La remémoration des temps longs nous invite à considérer que le risque était bien moins connu dans le passé, cela n'empêchait pas l'action et la prise de risque. De même, dans nombre d'autres cultures que celles des pays occidentaux, la vision du risque n'est pas la même. Dans nos sociétés, qui risque son intégrité physique ? Il n'en fut pas toujours ainsi. Un simple constat sur l'évolution récente de la considération du risque est celui de Tchernobyl. Repenser aux risques pris, à la catastrophe survenue, dans son ampleur et au fait que celle-ci n'a influée à l'époque que dans une moindre mesure sur la gestion des risques, amène à penser qu'aujourd'hui, il en irait tout autrement.

- **Les nouveaux champs de prise en compte du risque.**
  - ✓ **Pour un pilotage des risques émergents : Le management des risques suppose l'intégration d'un pilotage des risques émergents.**

La norme ISO 31000 (2009, Management du Risque, Principe et lignes Directrices) précise même « il convient que les processus de surveillance et de revue de l'organisme s'appliquent à tous les aspects du processus de management du risque afin…de pouvoir identifier les risques émergents ».

L'orientation est donc très clairement celle d'une intégration d'un pilotage des risques émergents, donc résolument tourné vers l'avenir.

Toutefois, la recherche sur ces risques émergents peine à suivre l'évolution technologique et l'une des limites évoquées est celle d'une méfiance vis-à-vis desdites évolutions.

Pourtant, les problématiques d'image de l'entreprise et de responsabilité des organisations (responsabilité des mandataires sociaux, RSE) font du pilotage des risques émergents un sujet incontournable, si ce n'est la preuve d'une politique de « bonne gestion » des risques.

Le processus de pilotage des risques émergents, tel qu'évoqué dans l'ouvrage Les risques émergents, un pilotage stratégique, peut alors se décrire comme tel :
-réévaluer les risques déjà identifiés au regard des problématiques actuelles et dont l'impact et la gravité s'en trouvent modifiés.
-identifier les nouveaux risques et les intégrer dans l'analyse de type menaces et opportunités (évaluation des enjeux, de la nécessité de les traiter ou non).
-intégrer les enjeux émergents dans la décision stratégique.
Le pilotage des risques émergents suit alors la présente méthode :

-Mise en place d'une veille afin de détecter les risques émergents. (Identification des risques et priorisation de ces derniers)

-Qualifier et quantifier les risques émergents (approche par scénarios, recours à des méthodes de type scénario du fait de l'insuffisance de données statistiques, évaluation chiffrée pour les risques faisant apparaitre une menace élevée) Sont alors pris en compte les dommages directs (dommages aux biens, actions en responsabilité) comme indirects (atteinte à l'image et à la réputation, perte d'exploitation).

-la gestion des risques émergents : par la mise en place d'action de réduction ou de transfert de risque (lorsque le chiffrage des coûts des sinistres potentiels dépasse le seuil d'acceptabilité toléré par l'entreprise).

Peuvent alors être arrêté certaines sources de risques de manière autoritaire (arrêt d'une activité à risque, sortie d'un marché). Un transfert partiel ou total peut être imaginé (assurance, alternative risque Transfer via les marchés financiers). Des moyens de prévention et de protection ainsi qu'une politique de communication sur les risques pourront encore être adaptés à ces risques émergents.

Ainsi, en matière de nanotechnologies, des formations devront être mise en place de même que les moyens de protection (contre l'explosion, l'atteinte à l'environnement, pour la protection des salariés et personnels divers) devront être adaptés. Ces moyens sont alors spécifiques (notamment en termes de maintenance, de stockage, de production et de manipulation desdits produits).

Il sera alors nécessaire non seulement de penser à la sécurité des installations et de l'environnement entourant le site de production, mais aussi à celle des sous-traitants, de toutes les parties prenantes de la Supply Chain ainsi que des clients in fine.

Pour ce qui est des outils, la méthode des scénarios a été évoquée. La cartographie des risques peut s'avérer là-encore pertinente (sous réserve d'adaptations visant à tenir compte des échelles d'impacts et probabilité de survenance propres aux risques émergents).

On voit donc la dimension prospective d'une gestion des risques axée vers la prise en compte des risques émergents. Tant dans les outils que dans la visée même d'une telle politique de risque, il est question de prendre en compte des types de risque s à venir, encore mal connus, mais pour lesquels l'entreprise souhaite apporter une réponse proactive et non simplement subir le changement. Gérer les risques émergents, non les subir potentiellement, telle est la réponse qu'un pilotage stratégique de ces derniers peut apporter.

Une telle démarche devrait s'affirmer au regard de l'évolution actuelle de la gouvernance d'entreprise davantage tournée vers la prudence (loi Sarbannes-Oxley, Loi de sécurité financière, le référentiel COSO II, la loi du 3 juillet 2008 afférant au renforcement de la communication et de la surveillance des risques…). De tous ces dispositifs prudentiels découlent une trame commune : celle selon laquelle il incombe, dans une visée éthique, aux conseils d'administration et comité de direction d'être les garants de la gestion des risques de leur entreprise. Ladite gestion des risques, stratégique de par ses impacts et prospective de par son regard résolument tourné vers l'avenir, ne peut en ce sens qu'être amenée à se développer.

Le dilemme de la réponse aux risques émergents :

Le pilotage de ces risques émergents implique un paradoxe : plus l'on repère tôt ces risques, plus les possibilités d'action sont importantes et efficace (mais celles-ci auront un degré d'incertitude non négligeable). A contrario, plus on avance dans la connaissance des risques, moins il est possible d'agir (le cas de l'amiante ou de catastrophes liées à des produits chimiques sont évocateurs à cet égard).

Une réponse face à ces risques peut consister à analyser les différentes solutions de traitement et de pilotage des risques émergents et leurs impacts.

Les solutions à privilégier seront celles qui seront les plus adéquates tout en maximisant la valeur d'option (possibilité de faire marche arrière).

<u>Exemple :</u>

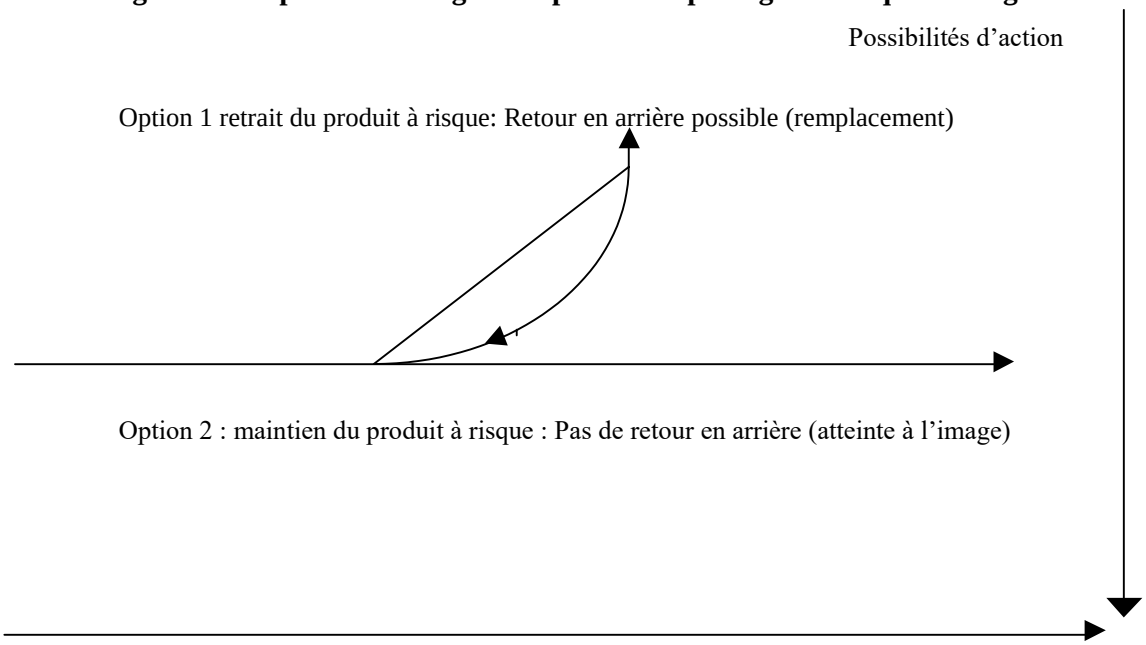
Option 1 : Retrait d'un produit sans forcément perdre un marché, remplacement de ce dernier

Option 2 : maintien du produit mais risque de dégradation de l'image de l'entreprise si l'essor des connaissances scientifiques révèle un risque émergent (non perçu auparavant).

Valeur d'option O1 > Valeur d'option O2

Le graphe des stratégies adaptatives est alors à cet égard un bon moyen pour se représenter les possibilités d'action évoluant dans le temps et celles pouvant permettre un retour en arrière ou non.

Figure 4: Graphe des stratégies adaptatives et pilotage des risques émergents.



4.2. La « prospective du risque », outils et approches méthodologiques :

L'intérêt d'une vision prospective pour gérer les risques ayant été étudié, il est question de voir dans quelle mesure les outils et méthodes de prospective peuvent trouver une utilité en gestion des risques.

Une mise en garde s'impose là encore. Pour des problèmes complexes, des méthodes simples et opérationnelles doivent pouvoir être mise en œuvre. Pour des problèmes simples, des analyses détaillées sont également pertinentes. Il n'est en effet pas aisé de réduire la complexité du monde et des risques qu'il comporte à un ensemble d'équations, de données, de variables, qui, par la combinatoire, peuvent donner un ensemble de résultats dont l'interprétation n'est alors pas toujours si éclairante pour le décideur. Concernant l'avenir, des modèles mathématiques complexes peuvent être rassurants mais ne se substitueront pas au jugement du décideur, preneur de risque, et présentent de nombreuses limites comme nous l'avons vu préalablement.

La prospective (anticipation pour éclairer l'action) se distingue de la prévision[43] (estimation du futur assortie d'un degré de confiance) en posant 5 conditions clés pour la

rigueur (pertinence, cohérence, vraisemblance, importance, transparence) permet de tendre aux futurs vraisemblables et souhaitables.

En ce sens, elle peut constituer de par son caractère méthodique un moyen d'amélioration des analyses de risques faites dans le cadre d'un processus de gestion des risques.

On distingue alors des méthodes objectives (exploratoires normatives), visant à décrire la réalité future sur la base de variables et d'indicateurs (exemple : la méthode des scénarios) et des méthodes subjectives. Ces dernières (intuitives) se basent tant sur les données que sur le savoir, l'expérience et l'intuition des experts (exemple : la méthode Delphi).

Comme le rappelle Michel godet (2002 : n°117), « les outils ne font pas les bons prospectivistes… », Leur utilité est de « stimuler l'imagination, réduire les incohérences, créer un langage commun, structurer la réflexion collective et permettre l'appropriation ».

Les outils seuls ne peuvent conduire au choix, ils peuvent structurer la réflexion mais ne sauraient la brider.

Ces conditions de rigueur ayant été passées en revue, il nous faut maintenant évoquer brièvement les outils de prospective pouvant trouver un intérêt en gestion des risques.

Les différents outils de prospective peuvent être utilisés de manière séquentielle. Toutefois, il est davantage question de voir les outils trouvant l'utilité la plus vraisemblable dans le cadre d'une démarche de gestion des risques tournée vers l'avenir.

✓ <u>La méthode des scénarios :</u> donner une image du risque et de ses conséquences.

« Un scénario n'est pas la réalité future, mais un moyen de la représenter en vue d'éclairer l'action présente à la lumière des futurs possibles et souhaitables. Les scenarios n'ont de crédibilité et d'utilité que s'ils respectent cinq conditions pour la rigueur : la pertinence des variables, la vraisemblance (on peut montrer que le scénario le plus probable n'a en général et au mieux que 15 chances sur 100 de se réaliser), l'importance des conséquences des scénarios et leur transparence ». (Est encore à ajouter la cohérence des éléments étudiés.) La méthode des scénarios trouve son intérêt afin de représenter des situations potentiellement réalisables. Cette méthode se trouve toutefois limitée en cas de contexte empreint de trajectoires multiples et incertaines ou de manque de connexité entre les variables. Il est alors nécessaire de recourir à plusieurs scénarios : Un scénario contrasté, un scénario catastrophe, un scénario optimiste.

On distingue également plusieurs catégories de scénarios : le scénario contrasté soit l'extrapolation d'un thème extrême (scénario par définition peu probable, par exemple une situation de crise majeure remettant en cause la pérennité d'une organisation, voir de la société elle-même : scénario de l'improbable), le scénario de référence (celui ayant le plus

de probabilité de survenir), le scénario d'anticipation (anticipation d'une situation future, exemple : anticiper la prochaine crue « centennale ») ou encore le scénario tendanciel (extrapolation d'une tendance).

Comme nous l'avons évoqué brièvement, l'utilité de la méthode des scénarios en gestion des risques est de scénariser les possibles en matière de risques et de catastrophes, voir de situations de crise. L'intérêt de cette méthode, couplée à l'analyse des jeux d'acteurs, à l'analyse des variables clés ainsi qu'à l'analyse morphologique, sera de permettre la construction de scénarios donnant une ou des images futures de situation à risque. Cela permettra encore, dans une optique de construction d'une cartographie des risques, de faire en sorte que cette dernière soit tournée vers les risques émergents et futurs et qu'il ne s'agisse pas uniquement d'une photographie du présent.

✓ L'analyse structurelle : est une méthode visant à recenser les variables d'un système, à établir des liens entre ces variables (matrice d'analyse structurelle) pour enfin identifier les variables clés.

Il peut s'agir d'une méthode efficace de construction d'un arbre de défaillance, d'un arbre des causes ou encore d'un arbre des évènements, ce en déterminant les variables clés, sources de risques dans l'organisation. L'utilité de cette méthode est encore de cibler les risques clés et de les prioriser et hiérarchiser en faisant ressortir ce qui est de l'ordre de l'urgence et de l'immédiat (moyen de se préparer aux crises et d'améliorer la réactivité).

On pourra alors se concentrer sur la catégorie des « variables risques » (pour déterminer par exemple les risques majeurs parmi les presque 500 risques de l'entreprise répartis en 13 classes, ou sur l'ensemble des variables de l'entité, tenté d'identifier les vraies sources de risques. Il y a donc plusieurs niveaux d'analyse possible.

A titre d'exemple, cela permet ainsi de se limiter à environ 70 variables réparties en catégories comme tel :

-variables organisation de l'entreprise et stratégie ;
-variables produits, marchés, technologies ;
-variables risques ;
-variables financières ;
-variables sociales ;
-variables distribution ;
-variables consommateurs ;
-variables générales.

Là encore, l'analyse structurelle peut être un moyen efficace de construire la base nécessaire à l'élaboration d'une cartographie des risques. Faire vivre cette cartographie est alors aisé. Il suffit de changer certains paramètres dans la matrice d'analyse structurelle pour obtenir des résultats actualisés. Le logiciel Micmac, par l'élévation en puissance de la matrice, permet aisément d'obtenir ces données ainsi que de déboucher sur des plans influence/dépendance entre les variables afin de voir les sources de risques et les entités potentiellement affectées par ces sources. Cela permet encore de voir (par l'analyse des plans influence/dépendance) si un système est stable (soumis à de nombreux risques ou non) et si les variables risques sont fortement influentes.

La dépendance des variables risques aux autres variables (exemple : processus de gestion des risques) permettra d'analyser le degré de maîtrise par risque et de manière générale (on peut donc même y trouver une utilité pour l'évaluation de l'efficacité des dispositifs de gestion des risques).

Pour des risques peu connus, peu maîtrisés, là où les statistiques font défaut, une telle utilisation peut apporter un éclairage intéressant.

Autre point, cette analyse des variables permettra de faire ressortir des constats sur la dépendance de l'entreprise plus ou moins forte à des risques externes (variables externes) ou internes (variables internes).

Enfin, autre utilité, en matière de repérage des signaux faibles de risque. L'analyse structurelle permet le ciblage de variables dites « cachées » (du fait de l'examen des effets directs et indirects de variables sur d'autres). Cela permet ainsi de voir encore si le fait d'apporter une solution à un risque ne sera pas la source d'autres risques (le processus de traitement des risques est donc bien sécurisant, par exemple : s'assurer que l'achat de moyens de protection incendie ne laisse pas démuni financièrement face à un autre risque tel que le risque de trésorerie).

On le voit donc, cette méthode est l'occasion d'obtenir un ensemble d'informations et d'éclairage sur l'entité en matière d'exposition au risque. Elle suppose toutefois une vision globale de l'entité, c'est pourquoi le lien avec le processus de gestion globale du risque apparait pertinent (visant à recenser et à cartographier les risques de l'entreprise dans une approche top-down et Botton-up).

Seule limite, une analyse structurelle est souvent un exercice long en pratique. Par conséquent, bien que pouvant faciliter la construction d'une cartographie des risques, sa pertinence pour faire évoluer cette dernière devra faire face aux contraintes de temps que l'organisation veut bien accorder à ces démarches. Par ailleurs cette méthode n'a pas pour

but de décrire un système de manière exhaustive, elle met en lumière des tendances ainsi que les facteurs déterminants au sein de l'entité pour le domaine étudié.

4.3. Formalisation d'une démarche de gestion prospective du risque :

Face au constat de certaines lacunes du Risk Management, de l'intéressante complémentarité que les méthodes de prospective pourraient apporter, et puisque l'avenir ne s'attend pas, mais se propose, Mr. Adrien Lebègue, étudiant en double diplôme ENASS-CNAM-LIPSOR) à proposer une méthode simple de gestion proactive du risque.

1- **La proposition :**

L'objectif est d'implémenter une « boîte à outils », à la fois simple et opérationnelle, traitant des aspects humains, organisationnels et comportementaux.

La simplicité et l'adaptabilité des outils aux sujets traités et dans le temps doit prévaloir. La proposition est donc celle d'une Méthode d'Analyse Prospective du Risque ciblant sur les Opportunités et Menaces affectant l'entité (MAPROM).

La démarche ne prétend pas être révolutionnaire ni changer ou remettre en cause les nombreuses approches efficaces existantes. Il est davantage question de reprendre le meilleur état de l'art dans plusieurs domaines que sont le Risk Management, l'analyse de risque et la prospective et de les combiner en une « synthèse créative » (Marc Giget) afin d'en faire ressortir des synergies par une méthode simple et efficace de prise en compte des risques émergents et futurs, voie principale d'amélioration de l'actuelle gestion des risques. Là encore, plus que la démarche en elle-même et les résultats en découlant, c'est la création d'une culture de l'anticipation des risques dans l'entreprise et d'une vision prospective face à ces derniers qui importent.

2- **La démarche et la méthode :**

Reprenant la démarche type « IVTS », nous proposons d'y décliner les éléments de l'analyse prospective selon ces différentes phases afin de les rendre plus pertinentes.

Ainsi, l'identification des risques se trouve facilitée par l'analyse des variables clés (analyse structurelle). Le balayage du champ des possibles (analyse morphologique) et les ateliers de prospective permettent d'élargir l'éventail des risques potentiellement réalisables et vraisemblables. Ce sont alors des moyens efficaces de construction d'une cartographie des risques tournée vers l'avenir. L'analyse des jeux d'acteurs (méthode MACTOR) permet de déterminer qui émet les risques, qui les subit et qui les assume in fine, ce qui permet de construire aisément les arbres d'évènements ou de défaillance.

Par ailleurs, l'horizon pertinent d'analyse du risque est repoussé (10 ans au lieu de 3 ans environ pour les démarches de type Risk Management). Un tel horizon permet ainsi de cerner de manière pertinente la majorité des risques émergents (voir schéma ci-dessous) et les principaux risques futurs susceptibles d'affecter l'organisation.

Au stade de l'évaluation des risques, face au manque criant, voire l'absence de données et de statistiques en matière de risques futurs, la réalisation de scénarios basés sur les éléments et avis d'experts récoltés au cours de la phase d'identification des risques (ne seront retenus que les scénarios probables et vraisemblables, notamment aidés par la méthode Smic-Prob-Expert) permettra de fournir une base de réflexion stratégique.

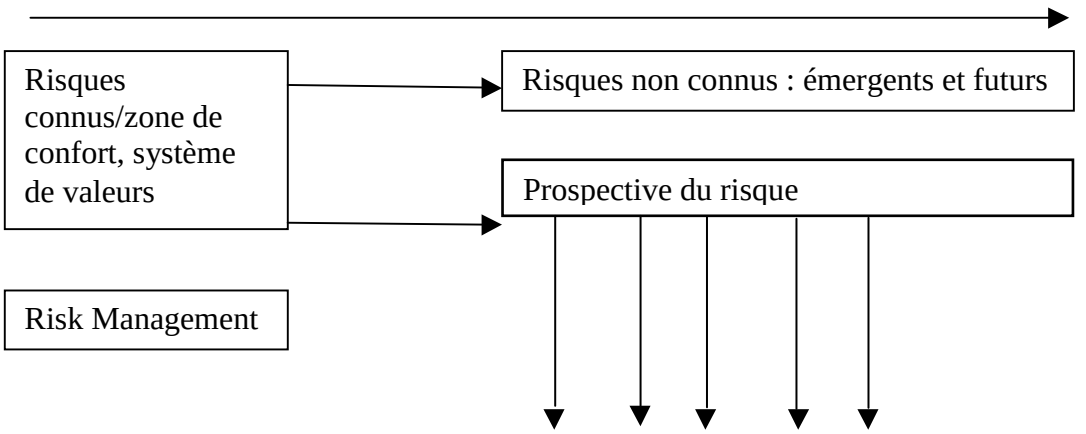
Sur cette base, seront alors priorisés et hiérarchisés des scénarios de survenance de risques. Une fois cette priorisation effectuée, des moyens de traitement et de suivi des risques pourront être mis en place. Pour le suivi des risques, des méthodes « classiques » sont suffisantes (reporting, veille…). Pour ce qui est du traitement, là encore, il sera question de choisir par exemple entre des moyens de protection, de prévention, de transfert de risque, ou un subtil arbitrage entre ces solutions. Afin de procéder au choix le plus efficace, la méthode Multipol, de choix et d'évaluation des options stratégiques peut permettre une prise de décision efficace. Elle peut permettre de mettre en lumière les sources réelles d'opportunités (sur lesquelles il faut se concentrer).

L'objectif étant donc de transformer les risques menaces en risques sources d'opportunités (Par exemple, la contrainte d'aggravation des évènements dommageables d'origine climatique peut constituer un signal fort de développement de la demande de couverture d'assurance et donc la nécessité d'innover pour créer et proposer des produits adaptés. Autre exemple, pour le risque de produit concurrent substituable : envisager des scénarios de nouveaux produits face à cette menace, procéder à une étude des nouveaux marchés afin de se défaire de la concurrence.)

3- L'implémentation : Méthode d'Analyse Prospective des Risques-Opportunités/Menaces(MAPROM).

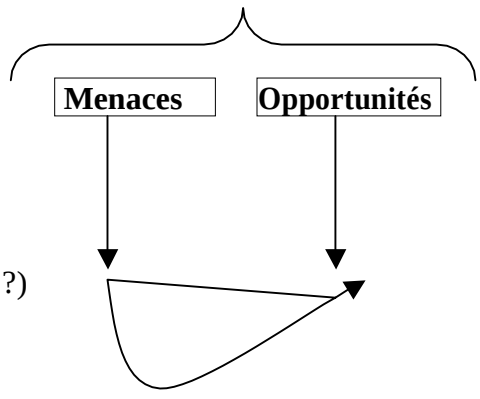
Figure 5: Méthode d'Analyse Prospective des Risques- Opportunités/Menaces (MAPROM)

Futurs possibles



Identification :
-Analyse des variables clés
-Ateliers de prospective
-Balayage du champ des possibles → Construire : Cartographie/ Plan Sévérité-Criticité
-Jeux d'acteurs → Construire : arbre des évènements/défaillances
(Qui émet le risque ? qui le subit ?)

Evaluation :
Réduire l'incertitude :
-méthode d'experts (smic prob-expert)
-méthode des scénarios



Traitement et suivi :
-Jeux d'acteurs (Qui assument le risque ?)
-Décision et choix multicritères :
(Multipol) (Exemple : Arbitrage prévention/protection
/Transfert du risque)

Remarque : A l'instar de la démarche intégrée de la prospective stratégique, il n'est pas obligatoire ni toujours nécessaire d'appliquer l'ensemble de la méthode. Ainsi, l'intérêt principal de la méthode MAPROM se situe davantage au niveau de l'identification et de

l’évaluation des risques.

Concernant les phases de traitement et de suivi des risques, les propositions faites peuvent être efficaces mais non indispensables. Par ailleurs, une telle méthode appelle des améliorations et développements : il ne s’agit ici que de proposer une piste de réflexion en matière de Prospective et de Risk Management, et de connexité des sujet et méthodes employées.

Conclusion de deuxième chapitre :

Parvenus au terme de ce chapitre, nous avons présenté dans la première section la revue littérature, et dans la deuxième section qui est subdivisée en deux sous-sections, la première sous-section nous avons la notion du système d’informatique. Ayant délimité notre travail aux risques informatiques, nous avons présenté les types de risques informatiques, les stratégies de mitigation, et les méthodes de gestion des risques telles que MADS-MOSAR. Et pour la deuxième sous-section nous avons présenté l’apport de l’implémentation de la prospective stratégique en gestion des risques.

CHAPITRE II : CADRE METHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

La validité de toute étude repose sur la méthodologie qui est suivie pour la conduire. En particulier, cette méthodologie concerne les démarches utilisées pour obtenir les principaux matériaux de l'étude, c'est-à-dire les données et les procédures relatives à leur traitement. Dans ce chapitre, deux sections existent. La première section consiste à voir le cadre méthodologique de la recherche, par ailleurs, nous allons examiner les raisons et les objectifs de choix de thème, le paradigme de l'étude, le choix du type d'étude, les instruments de mesure, la collecte des données et la méthode de traitement des données, la deuxième section nous allons présenter l'organisme d'accueil.

Section n°01 : La méthodologie de recherche

1. Les raisons et les objectifs de choix de thème :

On a choisis le thème « La mise en place d'une démarche prospective de gestion des risques au sein de la direction informatique de la (DGB) en utilisant la méthode MADS-MOSAR» pour plusieurs raisons :

- ✓ C'est un sujet intéressant qui conduit les responsables à chercher une politique pour assurer une gestion prospective des risques informatiques efficace dans l'organisation ;
- ✓ En plus, est un sujet d'actualité surtout avec le taux élevé des risques informatiques dans l'organisation ;
- ✓ Montrer le rôle de la prospection de gestion des risques dans l'anticipation des risques informatiques.

Nos objectifs principaux qui nous poussent à choisir ce thème :

- ✓ Maintenir un niveau élevé de motivation concernant le sujet ;
- ✓ Avoir des informations courantes sur le sujet ;
- ✓ Identifier, formaliser et implémenter des standards et des procédures de gestion des risques et former tous les acteurs à leur utilisation;
- ✓ Intégrer la dimension culture du risque lié aux SI dans l'élaboration de la cartographie des risques et sensibiliser la direction, le personnel de façon à favoriser l'émergence de cette culture et d'un cadre normatif de gestion de risque au sein de la direction informatique;
- ✓ Mettre en place un environnement adéquat (au sein des structures de gouvernance des SI) afin de contribuer au dialogue entre le service informatique, les directions métiers sur les aspects liés aux risques informatiques;
- ✓ Analyser le niveau de contribution actuel de gestion des risques dans la direction liés au système informatique afin de proposer des axes d'amélioration.

2. Paradigme de l'étude :

La démarche globale de cette recherche repose sur une approche hypothético-inductive en utilisant spécifiquement un paradigme constructiviste, reposant sur l'idée que notre image de la réalité, ou les notions structurant cette image, sont le produit de l'esprit humain en interaction avec cette réalité, et non le reflet exact de la réalité elle-même, selon Jean-Michel Besnier, (2005:p 44).

Selon Gauthier (1993 : p132), le chercheur « doit proposer une logique de démonstration des preuves qui permettra de voir si un dossier est favorable ou défavorable aux hypothèses construites ainsi que les significations que les gens attribuent à leurs expériences ». C'est pourquoi la perception des acteurs est sollicitée par des données fiables afin de faire une exploitation empirique de notre objectif principal de recherche.

3. Approche méthodologique :

Notre étude s'inscrit dans le cadre des recherches qualitatives en sciences de gestion. Elle est centrée sur une recherche-intervention unique au sein d'une organisation publique. La méthode qualitative nous a paru la plus appropriée dans la mesure où elle permet d'appréhender et de répondre à la question de départ, à savoir: Est-ce que la méthode MADS-MOSAR peut aider les gestionnaires pour assurer une meilleure gestion prospective des risques informatiques au sein de la direction informatique de la direction générale du budget ? La méthode qualitative nous permet par ailleurs, la prise en compte :

- De la richesse des mots employés par les acteurs de l'organisation. Comme le soulignent Huber man et Miles (1991), les mots possèdent un caractère «évocateur», « concret» et « significatif » qui s'avère plus convaincant que des «chiffres ».
- D'étudier des faits socioéconomiques à travers la documentation, les entretiens semi directifs et l'observation dans leur "milieu naturel".

Ces deux raisons nous ont permis de mieux cerner la complexité du phénomène à étudier. Quant au choix d'une recherche-intervention, comme stratégie de recherche, tel qu'elle est définie par Savall et Zardet (1995 : p104) « Cette recherche s'organise autour d'un processus d'interactivité cognitive entre les acteurs de l'entreprise et l'équipe de recherche », donc la RI consiste à aider, sur le terrain, à concevoir et à mettre en place des modèles, outils et procédures de gestion adéquats, à partir d'un projet de transformation plus ou moins complètement défini, avec comme objectif de produire à la fois des connaissances utiles pour l'action et des théories de différents niveaux de généralité en

sciences de gestion selon (Albert DAVID,2000), elle nous a semblé la plus appropriée pour aborder notre question centrale de recherche.

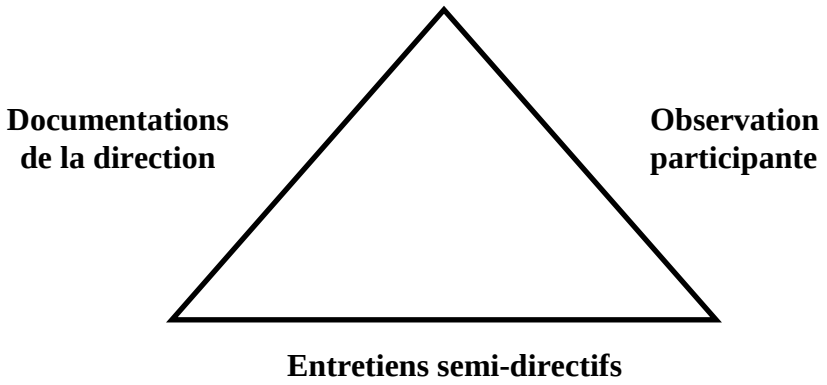
4. Délimitation du périmètre d'investigation :

Nos investigations sur terrain n'ont pas concerné toutes les structures de l'organisation. Notre choix était sélectif. Concrètement cela concernait la Direction Informatique (DI) qui s'occupe du système informatique au sein de la Direction Générale du Budget.

5. Recueil des données :

Pour mener à bien notre recherche, nous avons mobilisé trois approches, à savoir : l'observation participante, l'étude documentaire et les entretiens, que nous présenterons successivement selon le principe de triangulation.

Figure 6: Triangulation de trois principales sources de données (source nous-même)



5.1. L'entretien : est considéré comme principal mode de collecte de données primaires dans notre recherche. Selon (Thiétart et Coll 2007), « l'entretien est une technique destinée à collecter, dans la perspective de leur analyse des données discursives reflétant notamment l'univers mental conscient ou inconscient des individus». Nous avons opté pour l'entretien semi-directif ; qui permet de centrer le discours des acteurs interviewés autour de différents thèmes définis au préalable dans un guide d'entretien; avec les différents acteurs intervenants dans la gestion prospective des risques informatiques au sein de la Di y inclut les responsables de chaque sous-direction et chef de bureau.

5.2. L'observation participante :

L'observation est notre deuxième source de données. Elle peut être définie comme étant « une technique de collecte de données primaires visibles et audibles ». (Marie Laure et autre, 2008 p. 140).

Nous considérons que cette source d'information n'est pas une source de données mineur par rapport à l'entretien mais elle revêt toute l'importance nécessaire à la complémentarité

de nos données. En effet, l'objet de notre recherche qui est axé sur la gestion prospective des risques nous oblige à étudier ce dernier sur le vif de l'action.

Nos observations ont été réalisées au fur et à mesure de l'avancement de nos investigations commençant par l'observation des faits et des dires qui nous ont permis de formaliser notre problématique jusqu'à l'achèvement de notre études.

5.3. Collecte de documents:

La documentation est la troisième source de données que nous avons mobilisée, le rôle des documents consiste essentiellement à corroborer des informations et à augmenter la validité des autres sources.

Nos principaux supports documentaires sont : les sites, et les livres. Ensuite, après avoir entamé notre stage nous avons eu à consulter et à explorer des documents propres à l'établissement

En effet, la confrontation des trois sources d'information (l'entretien, l'observation et la documentation de la direction) nous permet de comparer entre ce qu'on dit (données issues des entretiens), ce qu'on fait (données issues de l'observation) et ce qu'on écrit (données issues de la documentation).

6. Les avantages et les obstacles de la recherche :

6.1. Les avantage :

Notre recherche effectue à la Direction Informatique de la Direction Générale du Budget, Ministère des Finances nous a permis de :

- Faire un aperçu dans le domaine de la recherche scientifique.
- Mettre en pratique les connaissances acquises durant notre cursus à l'école (ENSM), passer de l'aspect théorique à l'aspect pratique.
- Comparer entre le savoir scientifique acquit à l'école et la réalité de monde du travail de l'organisation.
- Bénéficier de savoir des cadres de la direction. Est ainsi l'occasion d'un apprentissage sur le comment faire.
- Permis d'acquérir des compétences dans la gestion et la présentation des données.

Mais son accomplissement n'a pas été facile, puisque durant notre enquête, on a rencontré un certain nombre d'obstacle.

6.2. Les obstacles :

- Au début de notre investigation, nous avons eu des difficultés pour avoir l'accès à une certaines directions. La demande de stage a pris plus de deux mois. Enfin on a décidé de retirer la demande pour aller à la Direction Informatique de la Direction Générale du Budget, ou les responsables nous ont acceptés facilement de faire un stage chez eux.
- la durée limitée du stage nous a contraints à faire l'impasse sur certains concepts que nous aurions pu approfondir d'avantage.
- la confidentialité des données à son influencé sur le niveau de détails perçu lors remplissages des questionnaires.
- Le manque des ouvrages qui traite notre thème.

Section n°02 : présentation de l'organisme d'accueil

1. Présentation du Ministère des Finances

Le Ministère des Finances est une institution qui joue un rôle très important dans l'économie nationale, il est composé de plusieurs directions générales liées aux domaines des ressources humaines, du domaine national, de la comptabilité, du trésor public, des impôts, etc. Cette composition est présentée au décret exécutif n° 07-364 de la 28/11/2007 portante organisation de l'administration central du Ministère des Finances.

1.1. Historique du Ministère des Finances :

Dès la constitution de l'Etat Algérien, à l'aboutissement des accords d'EVIAN en date du 06 avril 1962, ce dernier a procédé à la constitution de son gouvernement dont le Ministère des Finances.

De ce fait et au sein de cet exécutif, était prévue une Direction des Affaires Financière entièrement algérienne, et à l'application du décret n°1 de la République Algérienne Démocratique et Populaire a été nommé ministre des finances, le Docteur : AHMED FRANCIS.

Cependant, un décret est apparu le 4 septembre 1963 dont le but est le regroupement des administrations financières, de l'industrialisation et de l'énergie ainsi que la direction du plan et des études économiques pour donner naissance au ministère de l'économie nationale.

1.2. Attributions du Ministre des Finances :

Conformément au décret exécutif N°95-54 du 15 février 1995, le Ministre des Finances propose les éléments de la politique nationale en matière financière et en assure la mise en œuvre, conformément aux lois et règlements en vigueur.

Le décret exécutif N°95-54 fixant attributions du Ministre des Finances, stipule que « Le Ministre des Finances exerce ses attributions dans les domaines ci-après :

1. les finances publiques :
   -La fiscalité ;
   -La douane ;
   -Le domaine national et les affaires foncières ;
   -Les dépenses publiques, le budget et la comptabilité publique,
2. la monnaie ;
3. l'épargne, le crédit et les assurances économiques ;
4. les ressources du Trésor public ;
5. les interventions financières de l'Etat ;
6. la politique nationale en matière d'endettement extérieur ;
7. le contrôle des changes ;
8. le contrôle financier relatif aux utilisations des crédits du budget de l'Etat et des ressources du Trésor Public ;
9. les relations économiques et financières extérieures.

1.3. Organisation du Ministère des Finances :

Sous l'autorité du ministre des finances, l'administration centrale du ministère des finances comprend :

1.3.1. Le Secrétaire Général, auquel sont rattachés le bureau du courrier et le bureau ministériel de la sûreté interne, assisté de quatre (4) directeurs d'études et de trois (3) chefs d'études.

1.3.2. Le Chef de Cabinet : assisté de huit (8) chargés d'études et de synthèse, respectivement chargés :

- Des relations avec les instances législatives ;
- Des affaires juridiques ;
- Des relations avec les instances exécutives ;
- De la coopération internationale ;
- Des relations avec le mouvement associatif ;

- Des bilans et programmes d'activité du ministère ;
- Des dossiers inscrits aux conseils des ministres et aux conseils du Gouvernement ;
- Du suivi des réformes économiques et financières.

Et de six (6) attachés de cabinet.

1.3.3. Les structures suivantes :

- La Direction Générale de la Prévision et des Politiques (DGPP) ;
- **La Direction Générale du Budget (DGB);**
- La Direction Générale du Trésor (DGT) ;
- La Direction Générale des Impôts (DGI) ;
- La Direction Générale de la Comptabilité (DGC);
- La Direction Générale des Relations Economiques et Financières Extérieures (DGREFE);
- La Direction Générale du Domaine National (DGDN);
- La Direction Générale des Douanes, régie par un texte particulier (DG Douane) ;
- La Direction Générale de la Prospective (DGP) ;
- La Division des Marchés Publics (DMP) ;
- La Division des Investigations Fiscales (DIF) ;
- La Direction des Opérations Budgétaires et des Infrastructures (DOBI) ;
- La Direction de la Maintenance et des Moyens (DMM) ;
- La Direction des Ressources Humaines (DRH) ;
- La Direction du Système d'Information (DSI);
- La Direction de l'Agence Judiciaire du Trésor (DAJT) ;
- La Direction de la Communication (DC) ;
- L'Inspection Générale des Finances, régie par un texte particulier (IGF).

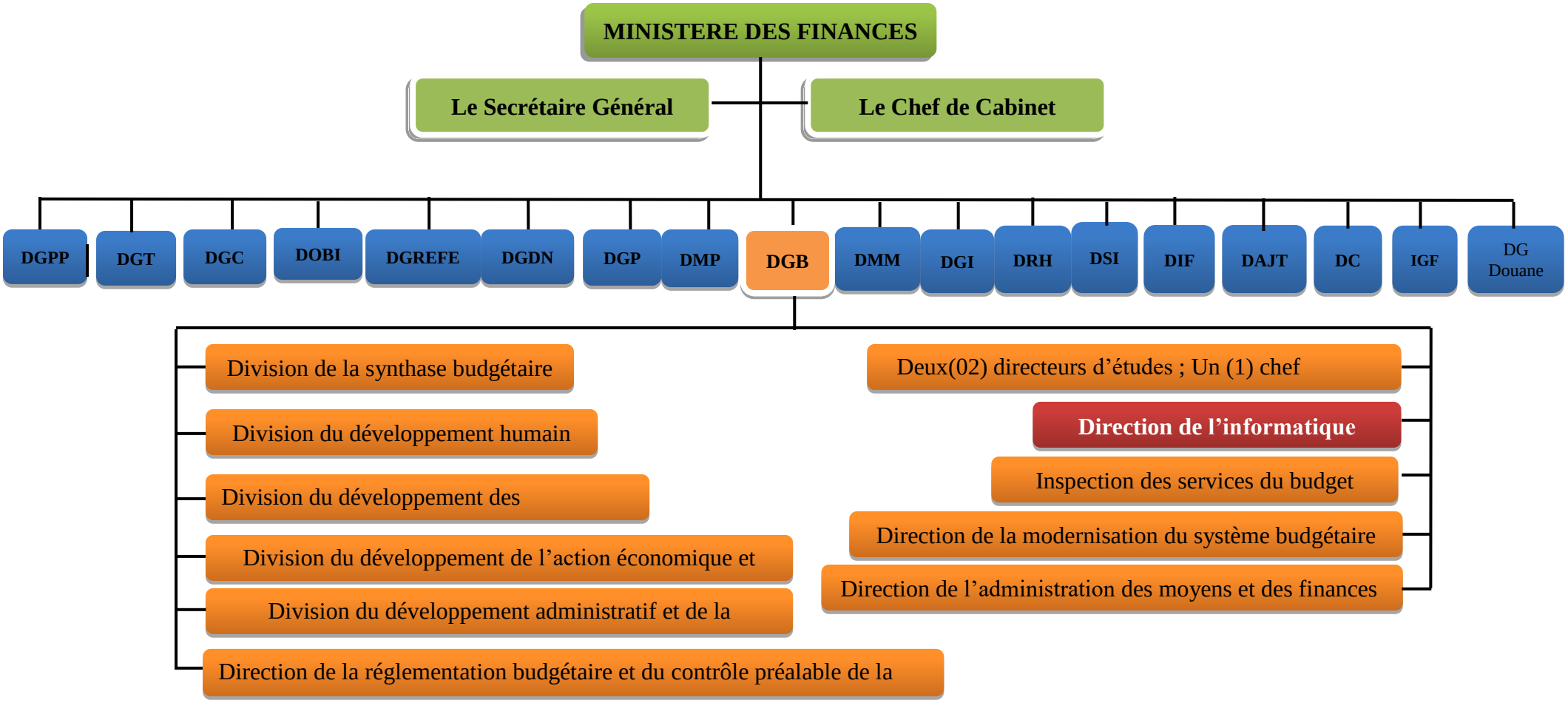


Figure 7: Organigrammes du Ministère des Finances (source : nous-mêmes, selon décrit exécutif n° 07-364)

2. La Direction Générale du Budget:

2.1. Présentation et fonctions :

La Direction Générale du Budget est l'une des neuf directions générales que compte le ministère des finances, elle est Chargée :

- De participer, en relation avec les structures et institutions concernées, à l'élaboration de la politique budgétaire.
- D'initier tout texte législatif ou réglementaire relevant de son domaine de compétence.
- D'étudier et de proposer toute mesure nécessaire à la normalisation des dépenses de l'Etat et à l'amélioration de leur efficacité.
- D'élaborer le projet du budget.
- D'assurer la mise en œuvre et le suivi de l'exécution du budget, de son contrôle et de son évaluation.
- De procéder à l'ouverture, à la transformation, à l'annulation et au redéploiement des postes budgétaires des institutions et administrations publiques.
- De participer, en ce qui la concerne, à l'étude, à la préparation et à la mise en œuvre des conventions et accords internationaux ayant une incidence financière sur le budget de l'Etat.
- De suivre la réforme budgétaire et de la mettre en œuvre.

2.2 Administration centrale : La Direction Générale du Budget est composée de :

2.2.1. Cinq (5) divisions :

- ✓ Division du développement humain ;
- ✓ Division du développement de l'action économique et sociale ;
- ✓ Division du développement administratif et de la régulation ;
- ✓ Division du développement des infrastructures ;.

2.2.2. Quatre (4) directions : selon le Décret exécutif n° 07-364 du 28 novembre 2007

- ✓ Direction de la réglementation budgétaire et du contrôle préalable de la dépense ;
- ✓ **Direction de l'informatique ;**
- ✓ Direction de l'administration des moyens et des finances ;
- ✓ Direction de la modernisation du système budgétaire.

2.2.3. Une (1) inspection : selon le Décret exécutif n° 08-154 du 26 mai 2008.

- ✓ Une inspection des services du budget.

2.2.4. Trois (3) assistants du Directeur Général :

- ✓ Deux directeurs d'études ;
- ✓ Un (1) chef d'études.

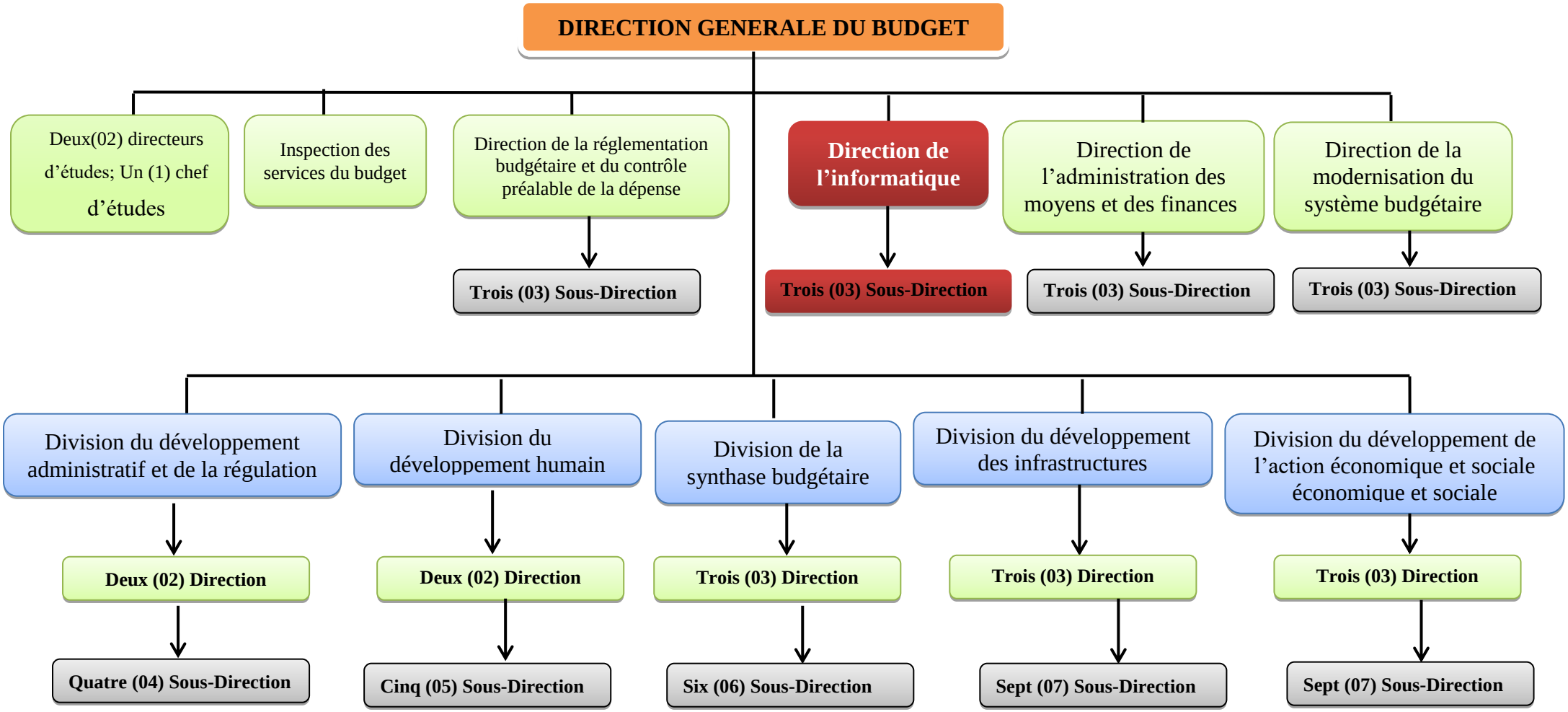


Figure 8: Organigramme de la Direction Générale du Budget (source : nous-mêmes, selon le décret exécutif n°07-364)

3. La Direction Informatique :

- De mettre en œuvre le schéma directeur informatique de la direction générale ;
- D'assurer le développement des applications informatiques ;
- D'assurer la maintenance des équipements informatiques, selon le Décret exécutif n° 07-364

Elle est composée de trois (3) sous-directions :

3.1. Sous-direction du développement des systèmes informatiques : Est chargée :

D'assurer le développement des applications spécifiques aux structures de la direction générale.

Elle est aussi bien composée de deux (02) bureaux :

a) Bureau du système d'information ;

b) Bureau du développement des applications.

3.2. Sous-direction du développement des Réseaux :Est chargée :

- De concevoir et de développer la plate-forme réseau ;
- D'administrer les bases de données et de gérer le réseau de la direction générale.

Elle est aussi bien composée de deux (02) bureaux :

a) Bureau d'administration du réseau ;

b) Bureau d'administration des bases de données.

3.3. Sous-direction de la maintenance des équipements et des logiciels :Est chargée :

- De configurer et d'assurer la maintenance des logiciels et des équipements ;
- D'évaluer les besoins en fournitures informatiques.

Elle est aussi bien composée de deux (02) bureaux :

a) Bureau de la maintenance des équipements ;

b) Bureau de la maintenance des logiciels.

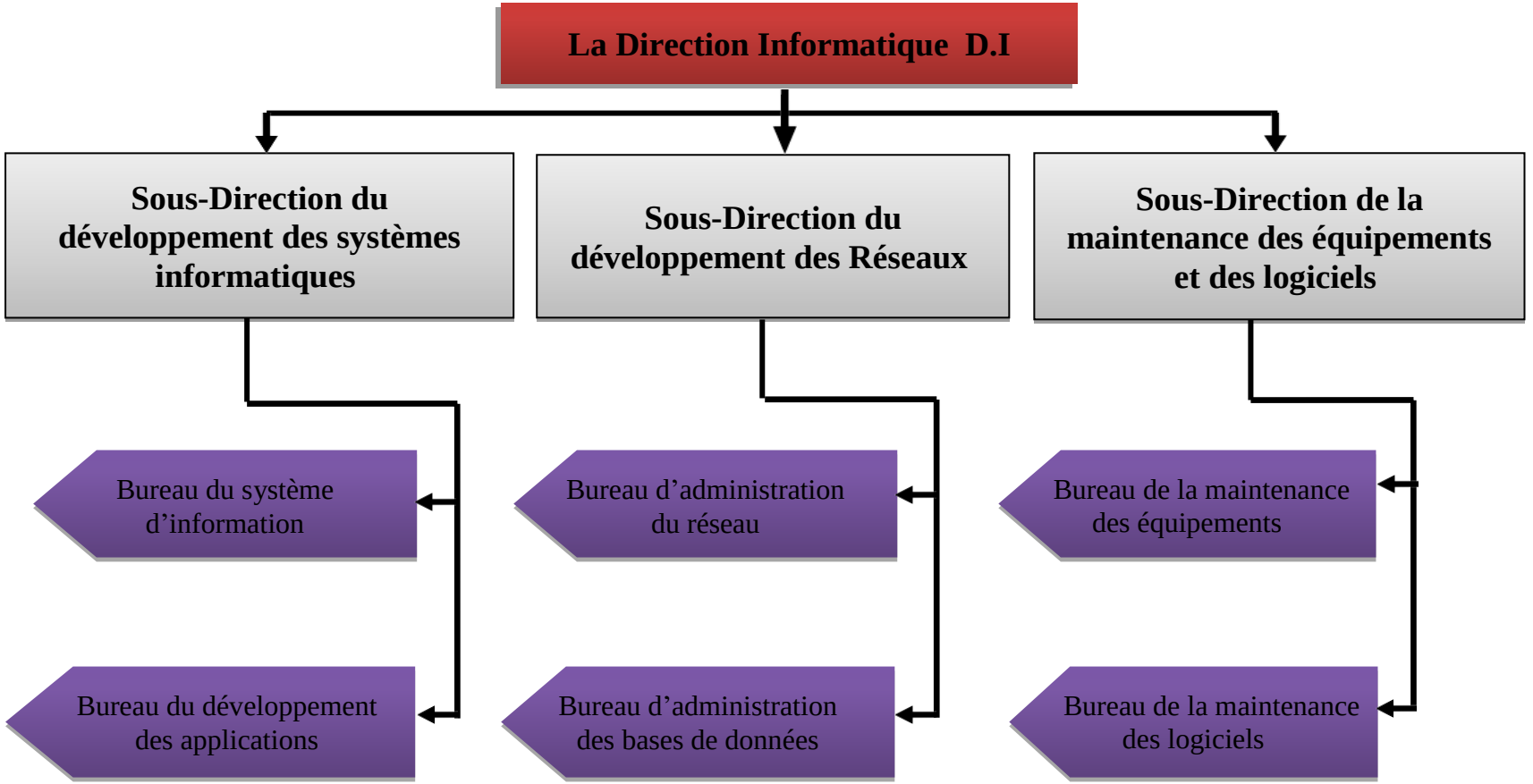


Figure 9 : Organigramme de la Direction Informatique (source : nous-mêmes, selon le décret exécutif n°07-364 du 28/11/2007 et l'Arrêté interministériel J.O n°24 du 14/04/2010)

CHAPITRE III : ANALYSE DES RESULTATS A L'AIDE DE LA METHODE MADS-MOSAR

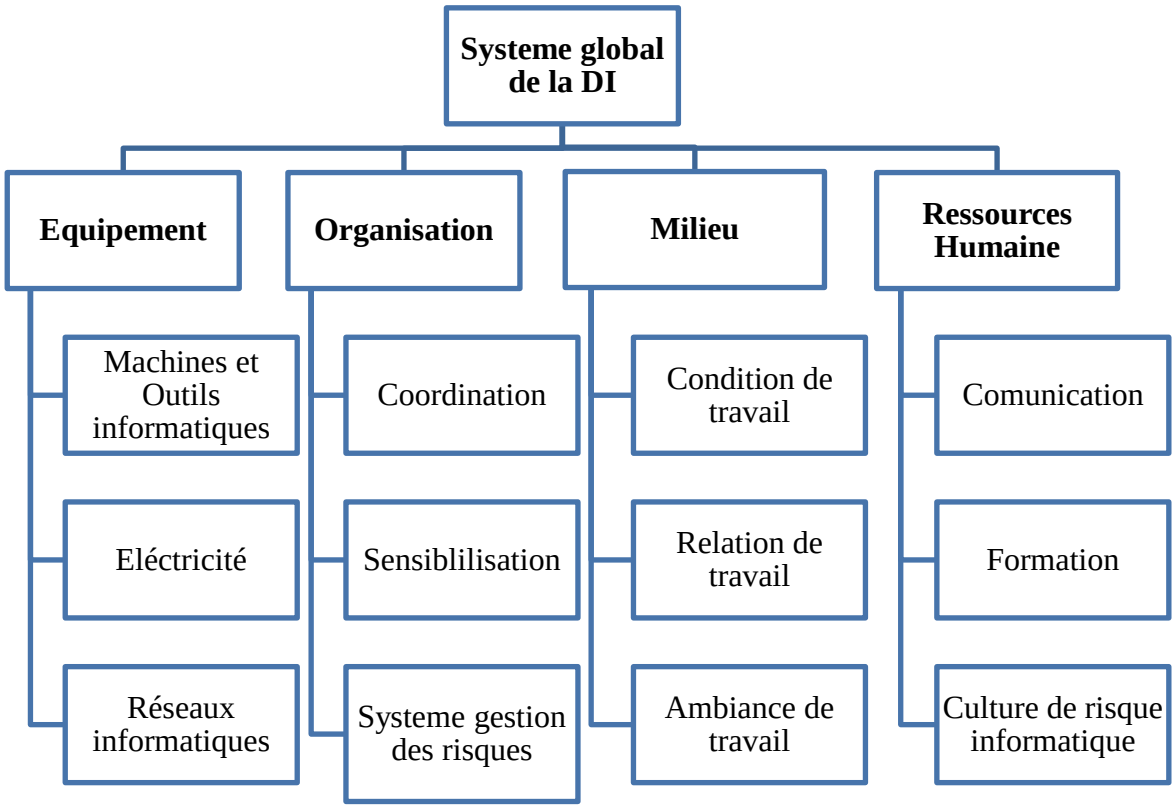
Dans ce chapitre, nous allons essayer d'appliquer la méthode MADS-MOSAR citée dans le chapitre 01, comme une méthode de gestion prospective des risques au sien de la direction informatique de la DGB, afin d'identifier en deuxième étape des scénarios possible des risques et les barrières de prévention et de protection en troisième étape dans le but d'optimiser l'efficacité du système informatiques.

1. Modélisation du système étudié en le découpant en sous-systèmes :

Afin d'identifier les sources de danger, il faut modéliser notre système globale «de la Direction Informatique» en sous-système peuvent devenir source de danger.

Nous avons découpé le système global de la direction informatique, en 4 sous système susceptible comme système source de danger pour l'activité comme il est schématisé dans la figure suivante :

Figure 10: Décomposions du système global de la direction informatique en sous-systèmes



Source : nous-mêmes, selon la documentation de la DI

Afin d'expliquer au mieux notre découpage, nous allons donner des petits définitions des quatre sous-systèmes identifiés. Ensuite nous avons élaboré un tableau pour classer les sous-systèmes avec leurs éléments.

- **Equipement** : le sous-système équipement compromet tout équipement sources de danger dans la sécurité : c'est selon les machines-outils, les outils, le parc informatique, les logiciels, etc.
- **Organisation** : le sous-système organisation implique toutes les actions importantes qui peuvent être la cause d'un dysfonctionnement du système informatique.
- **Milieu** : le sous-système milieu correspond généralement à l'environnement, mais qui peut aussi être compris davantage comme le contexte d'un moment. Les conditions de travail, l'ambiance et les relations de travail, les contacts entre les acteurs du réseau à l'intérieur du système ou avec d'autres systèmes font aussi partie du milieu.
- **Ressources humaine** : le sous-système ressources humaines implique toute action humaine qui peut être comme source de danger exemple : « absence de cultures de risque informatiques »

Sous système	Nom du sous système	Elément du sous système
SS1	Equipement	Machines et Outils informatiques
		Électricité
		Réseaux informatiques
SS2	Organisation	Coordination
		Sensibilisation
		Système gestion des risques
SS3	Milieu	Condition de travail
		Relation de travail
		Ambiance de travail
SS4	Ressource Humaine	Communication
		Formation
		Culture de risque informatique

2. Identifier les scenarios de dangers :

A travers les entretiens effectués avec les ingénieurs de système informatiques risques de la Direction Informatique **(voir Annexe VI, page 90)**, il s'est avéré que les scénarios des risques informatiques sont connus notamment grâce au retour d'expérience sont oublie l'observation mené au cours de processus, ainsi qu'à travers la base de données de la direction.

Les scénarios des risques qu'on va les identifiés regroupes les causes de danger les plus mentionnés par les employés dans les entretiens que nous avons distribué.

2.1. Identification des processus :

Dans cette étape on considère chaque sous-système cité dans le tableau02, comme un processus dont les entrées sont les événements initiateurs d'origine interne ou externe et les sorties sont les événements principaux qui peuvent déclenchés un risque.

2.2. Identification des scénarios courts :

Apres avoir identifié un processus pour chaque sous-système, l'étape suivante consiste à identifier des scénarios courts pour chaque sous-systèmes à travers l'association d'un ensemble d'évènements initiateurs et évènements principaux qui peuvent augmentés la probabilité d'un risque.

NB : Pour faciliter la lisibilité des scénarios retenue nous avons choisi de représenter les événements sous forme linaire et de donner une couleur pour chaque scénario afin d'éviter toute confusion dans la lecture des scénarios.

Dans les figues ci-dessous (figure 11 à 14), nous allons schématiser l'ensemble des processus et des scénarios court identifiés pour chaque sous-système.

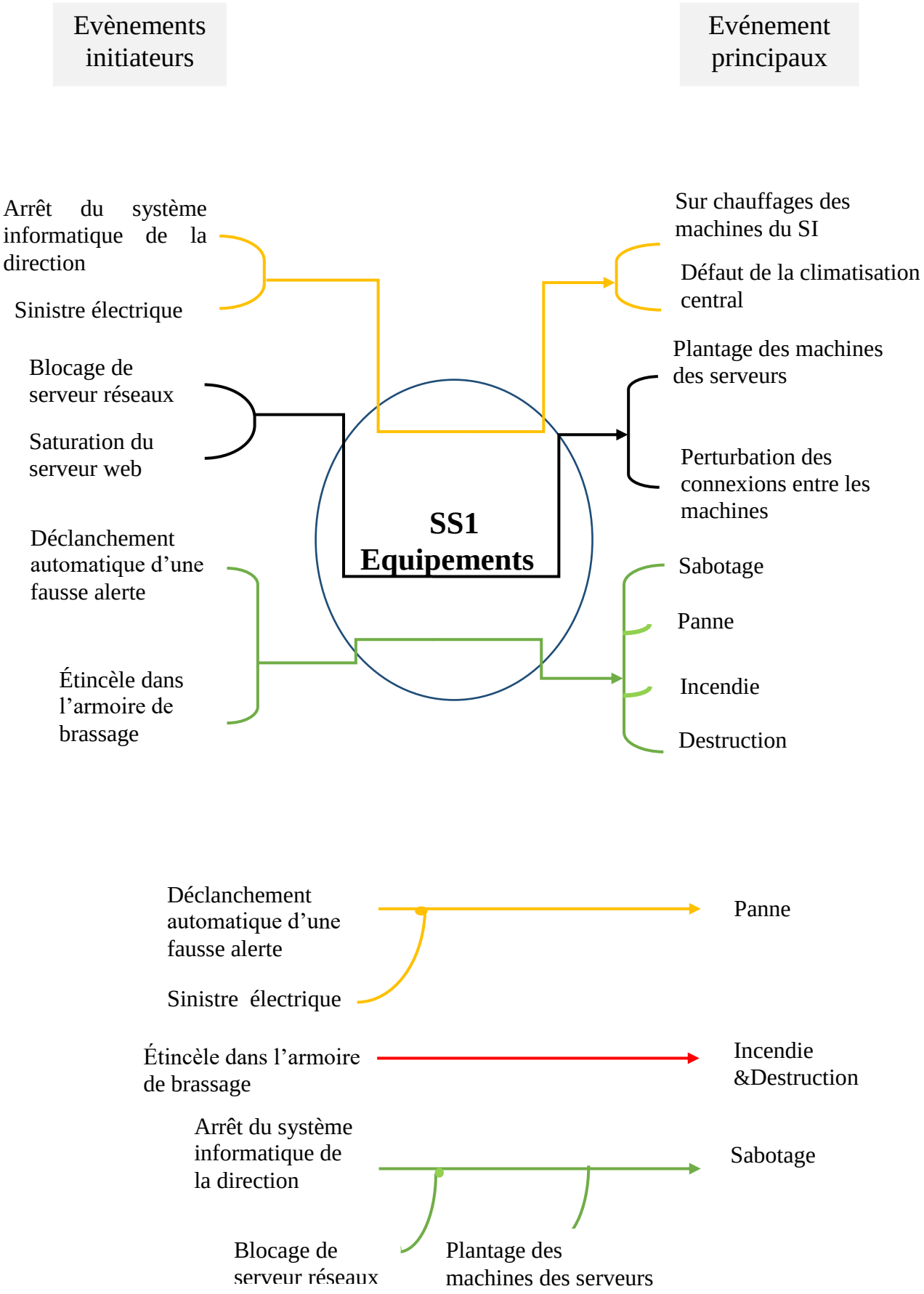


Figure 11: Scénario court du SS1 Equipement

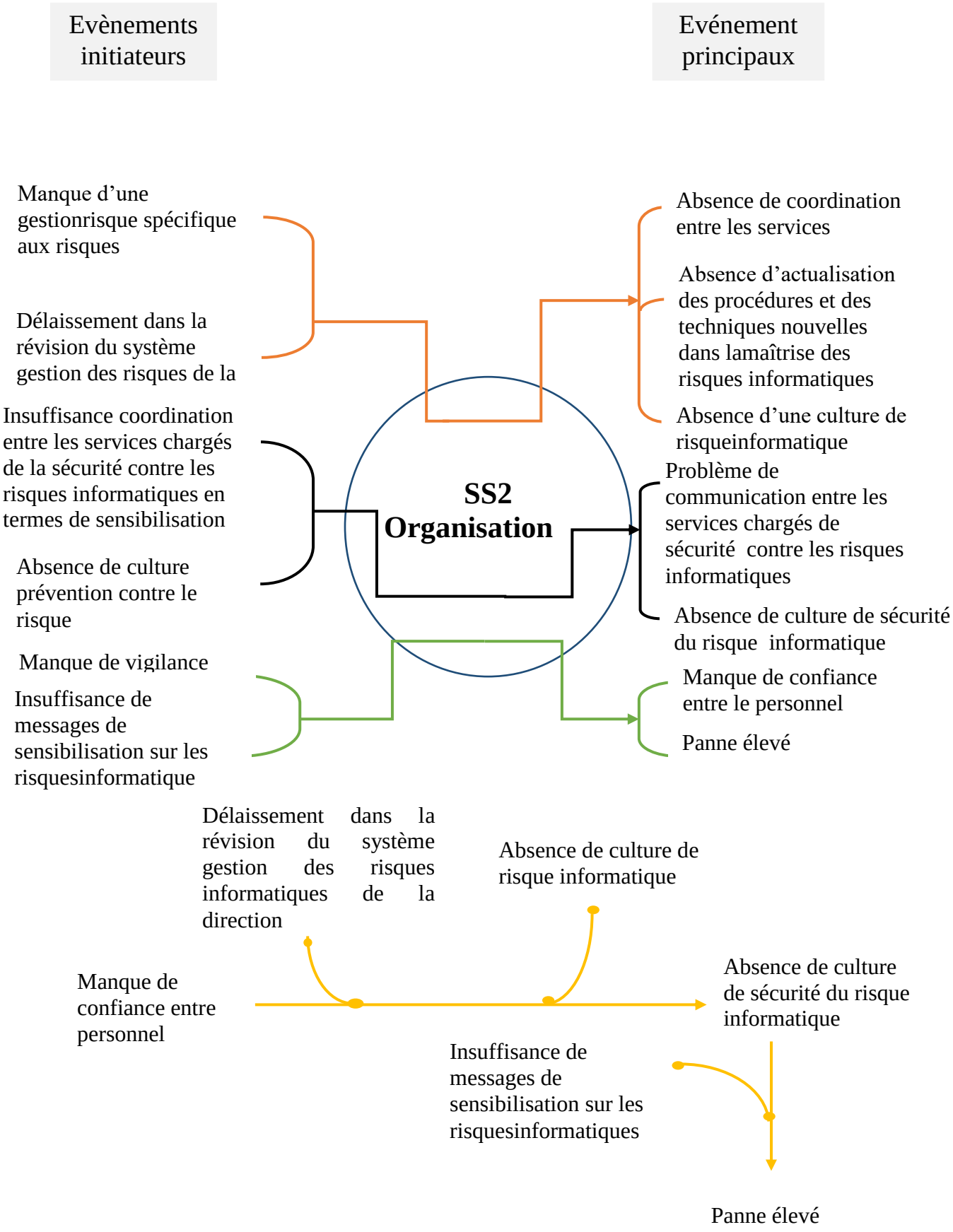


Figure 12: Scénario court du SS2 Organisation

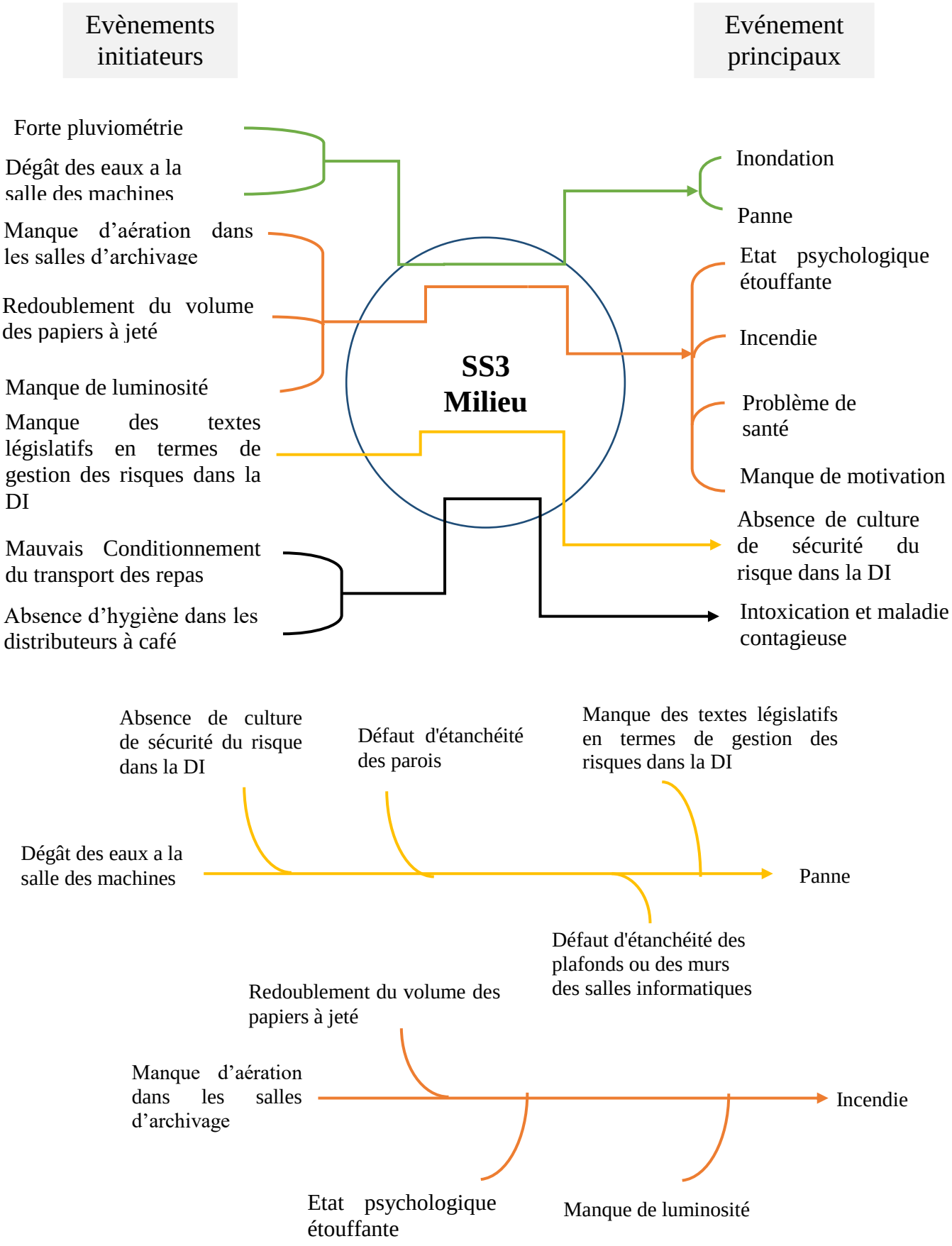


Figure 13: Scénario court du SS3 Milieu

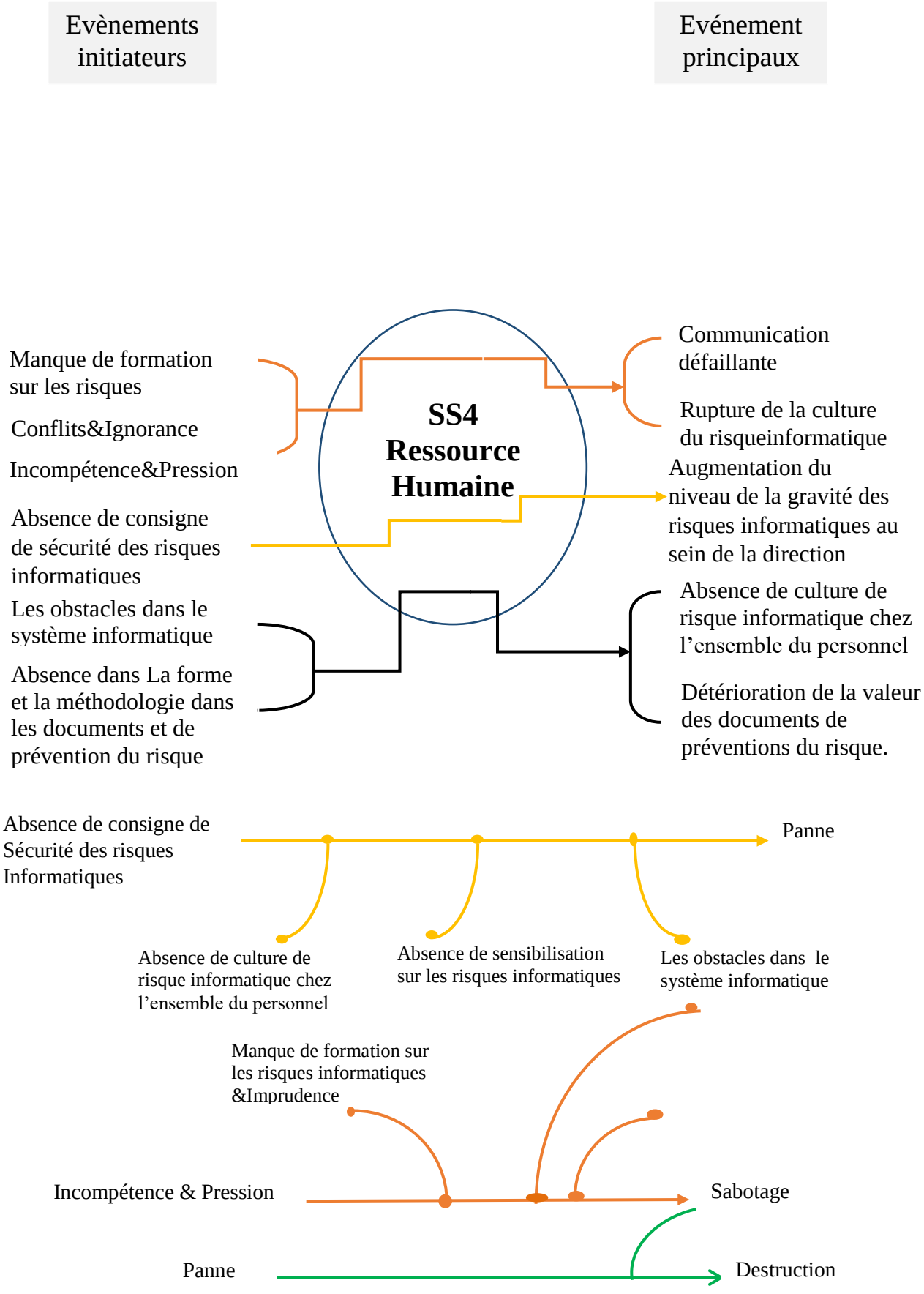


Figure 14: Scénario court du SS4 Ressources humaine

2.3. Identification de scénarios longs et construction d'arbres logiques:

D'après Jacquiot (2010), cette étape consiste à regrouper l'ensemble de processus des sous-systèmes afin d'observer toutes les interactions possibles des évènements incitateurs et les évènements principaux dans un système global dont on peut facilement identifier à la fin des scénarios longs pour le système comme il est représenté dans la figure 15 ci-dessous.

À partir des scénarios longs et des scénarios courts on peut construire aussi un arbre logique qui montre d'une façon progressive les relations direct et indirect des possibles des évènements incitateurs et les évènements principaux avec l'accident enregistré. Pour notre système on a rassemblé l'ensemble des scénarios identifiés pour l'ensemble des sous-systèmes pour qu'ils nous permettent de construire des arbres logiques pour trois principaux événements à savoir :

- Risque incendie
- Risque de panne
- Risque de sabotage

D'après l'observation menée, un événement initiateur peut déclencher d'autres évènements qui peuvent conduire à identifier d'autres scénarios.

Les scénarios retenus nous permettent d'évaluer qualitativement les événements, leurs impacts afin de pouvoir dégager à la fin des solutions comme des barrières de prévention et de protection aidants à renforcer le système de gestion prospective des risques au sein de la Direction Informatique.

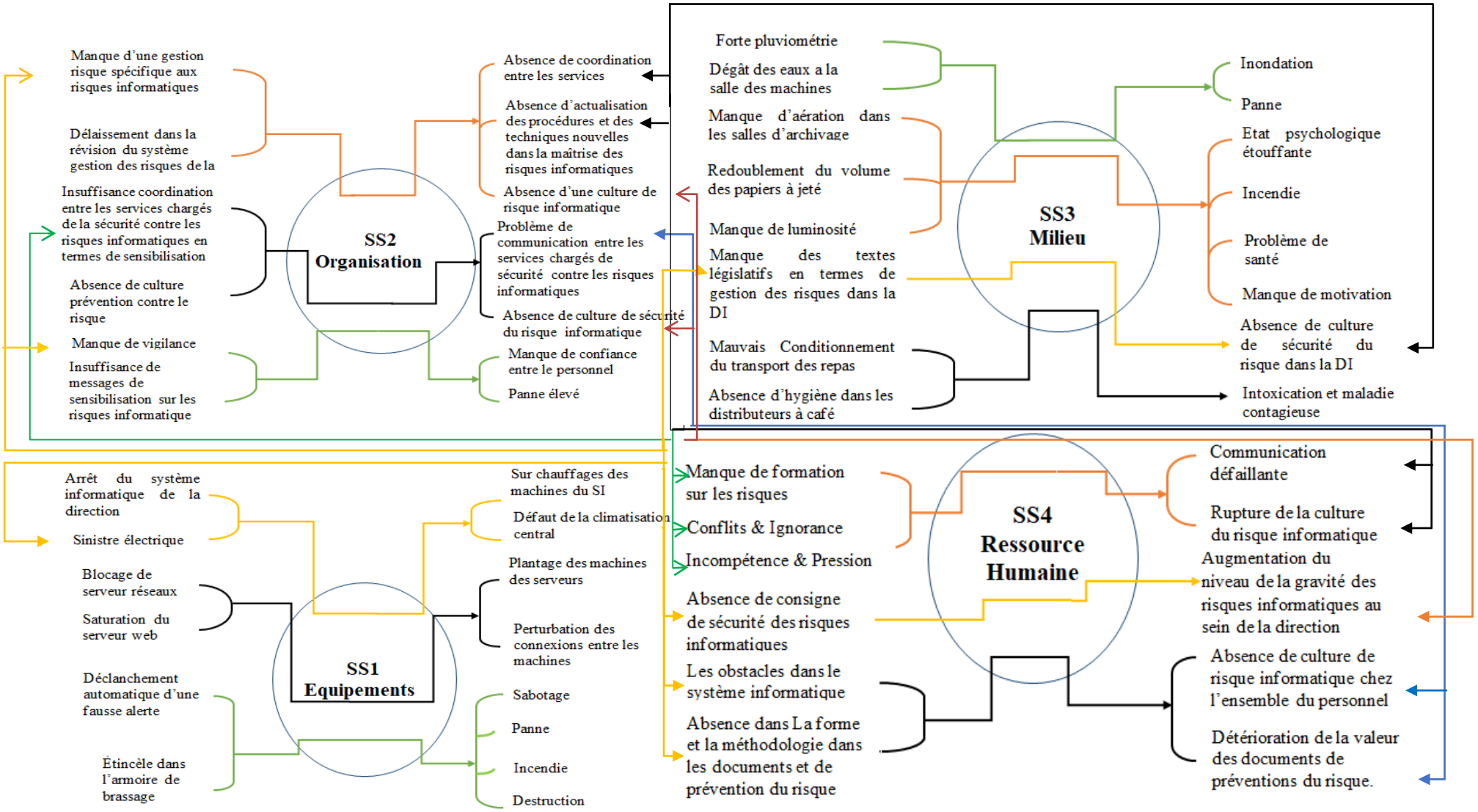
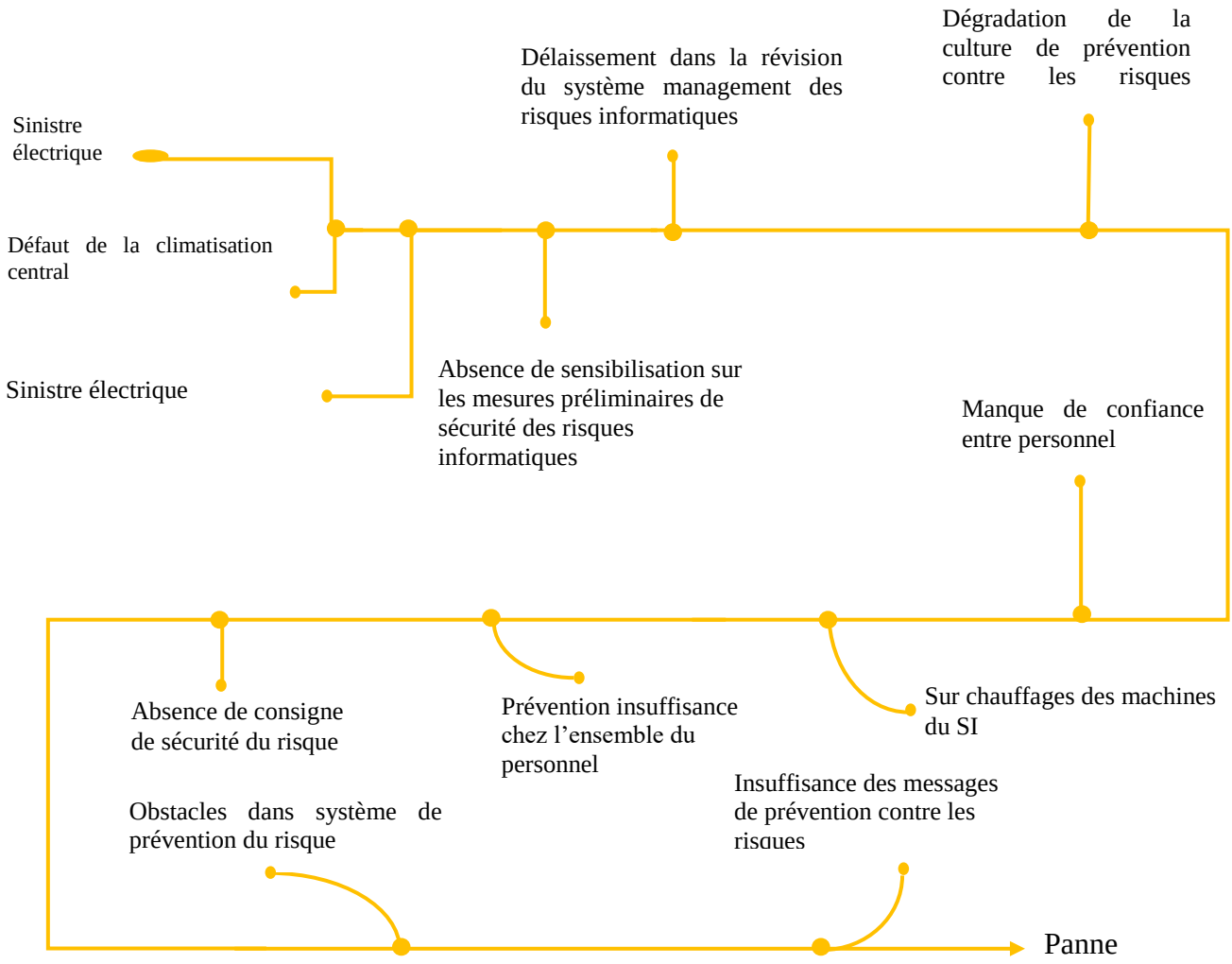
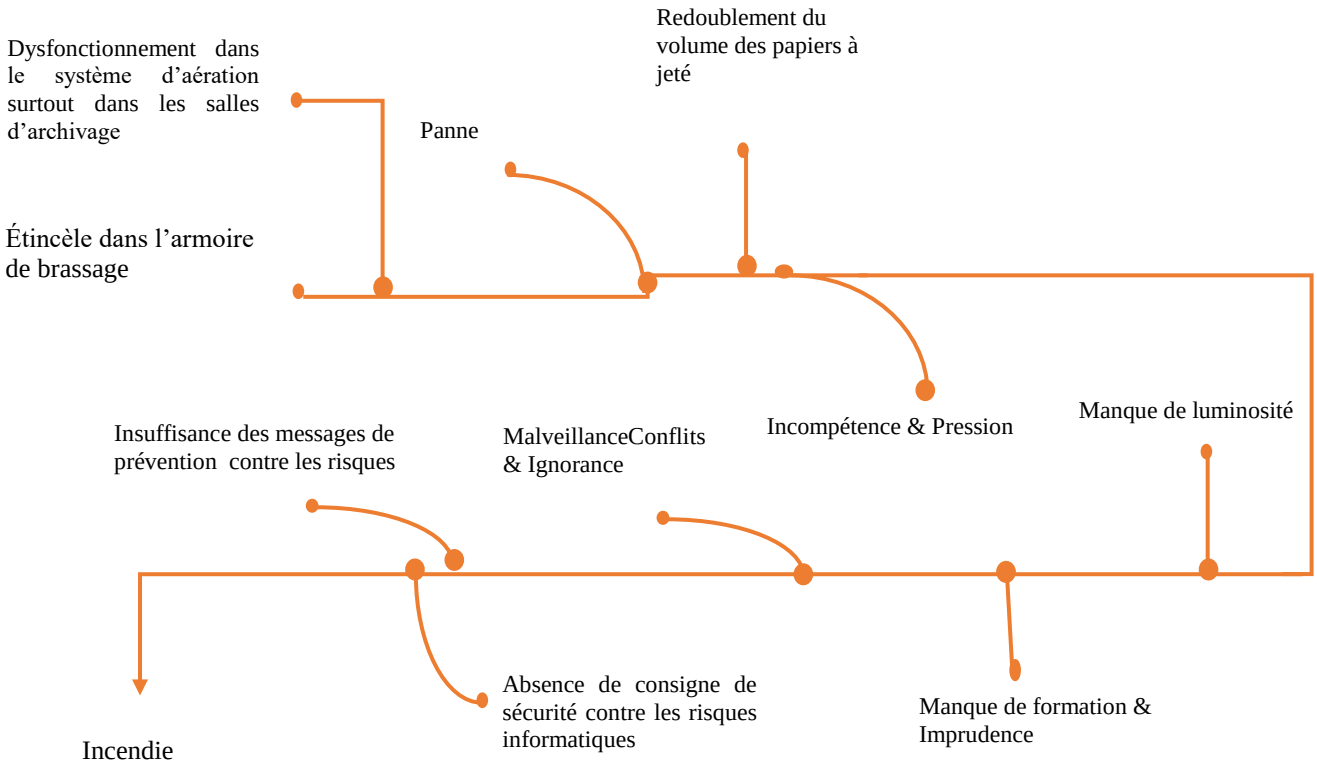


Figure 15: l'ensemble des processus du système de la « DI »

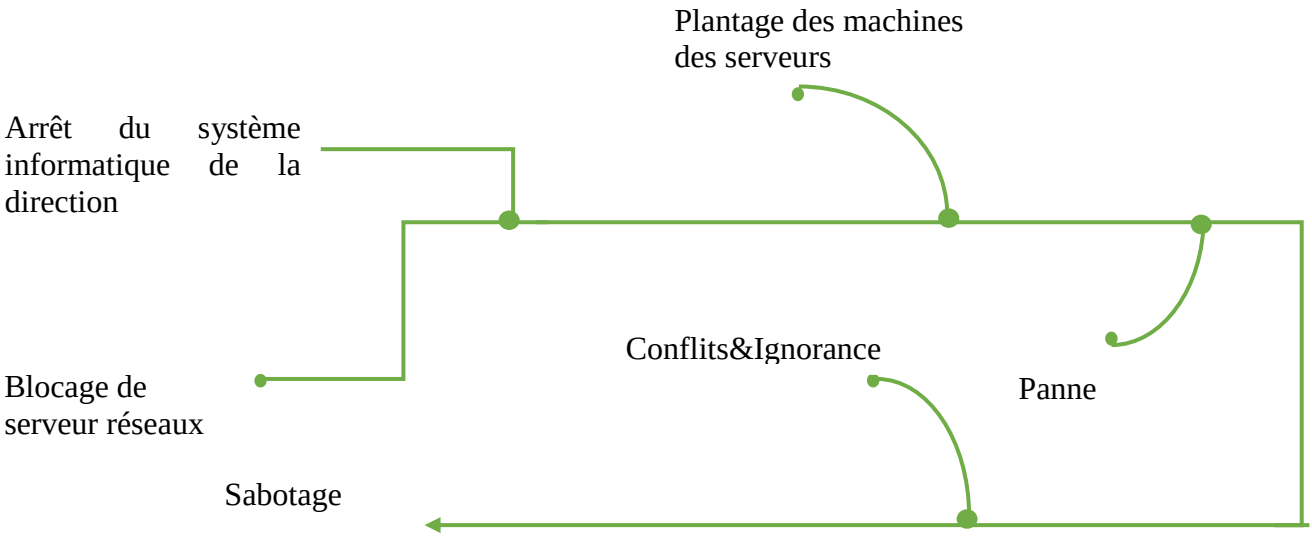
Scénario long S1 : Panne



Scénario long S2 : incendie



Scénario S3 : Sabotage



3. Évaluation des scénarios longs retenus :

D'après Jacquiot (2010), cette étape consiste à évaluer quantitativement et qualitativement les événements à l'aide d'un logiciel, un travail de groupe ou à travers le jugement d'experts.

On raison de l'absence d'un logiciel pour évaluer les risques, nous avons ressui avec un travail avec les tuteurs à évaluer l'impact et le degré d'occurrence de chaque scénario sur l'intégrité du système.

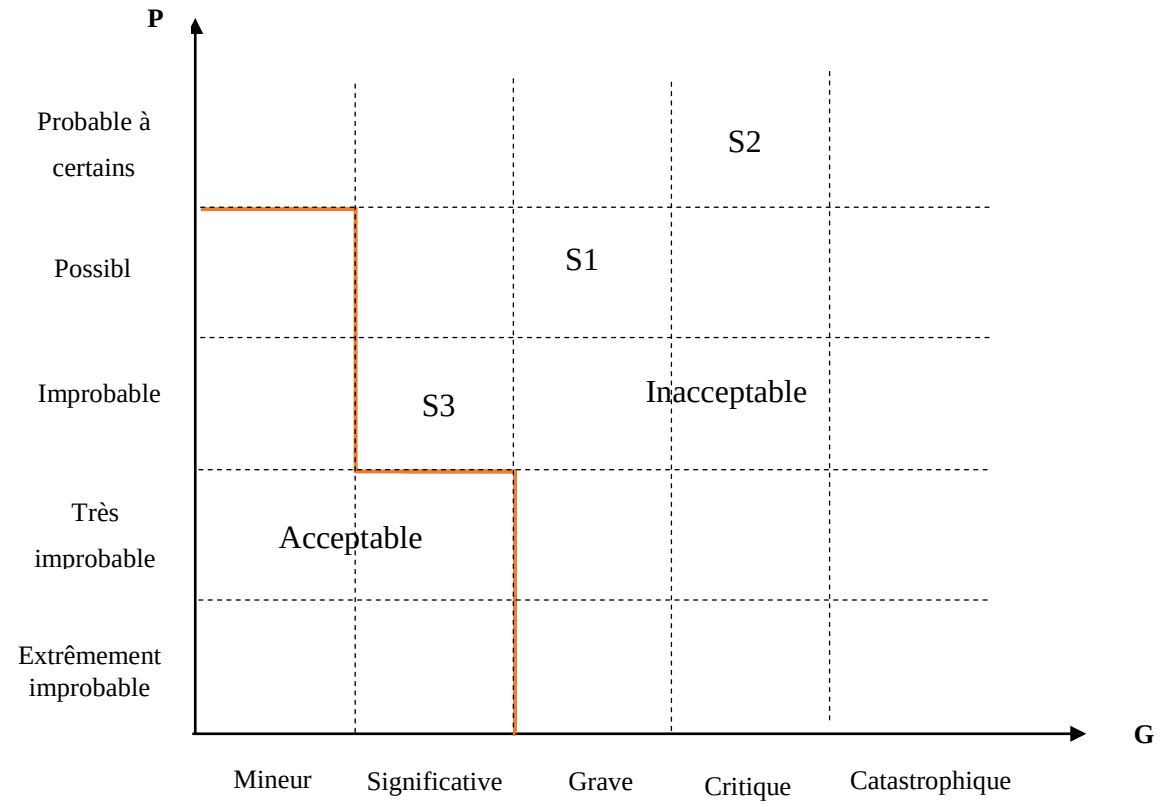
Selon Jacquiot (2010), il est nécessaire aussi identifier et analyser les cibles qui peuvent les événements principaux les atteindre et évaluer leurs impacts sur ces cibles. L'atteinte des cibles ainsi que leur nature dépend aux caractéristiques de l'évaluation des scénarios et la distance entre les événements finaux (P. Perilhon 2012).

Dans certains cas, la gravité est définie en fonction du scénario, car les scénarios se distinguent entre eux par leurs probabilités différentes. Cela nous permettra de calculer probabilités des scénarios retenus pour pouvoir proposer à la fin, une grille permettant de hiérarchiser les scénarios comme nous allons voir dans l'étape suivante.

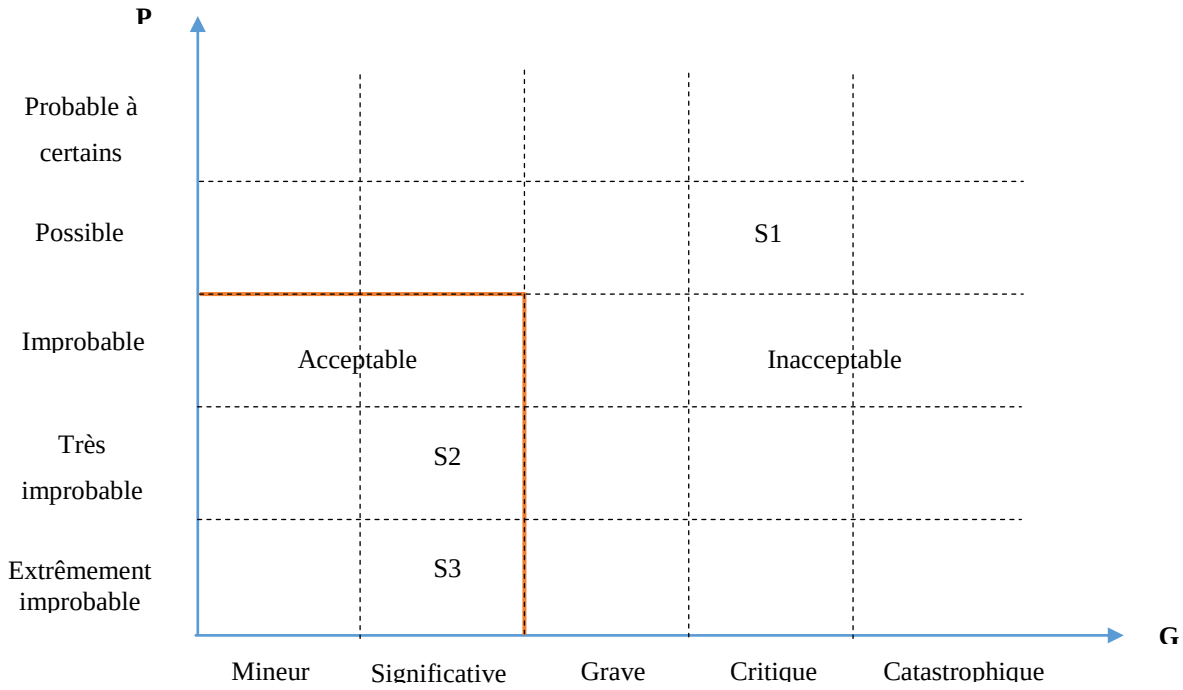
4. Négociation d'objectifs et hiérarchisation des scénarios :

Afin de négocier les objectifs et hiérarchiser les scénarios, il est nécessaire d'analyser et d'évaluer les scénarios courts de chaque sous-système selon leur échelle de gravité et probabilité afin de pouvoir définir le niveau de la criticité de chaque scénario dans chaque sous sous-système.

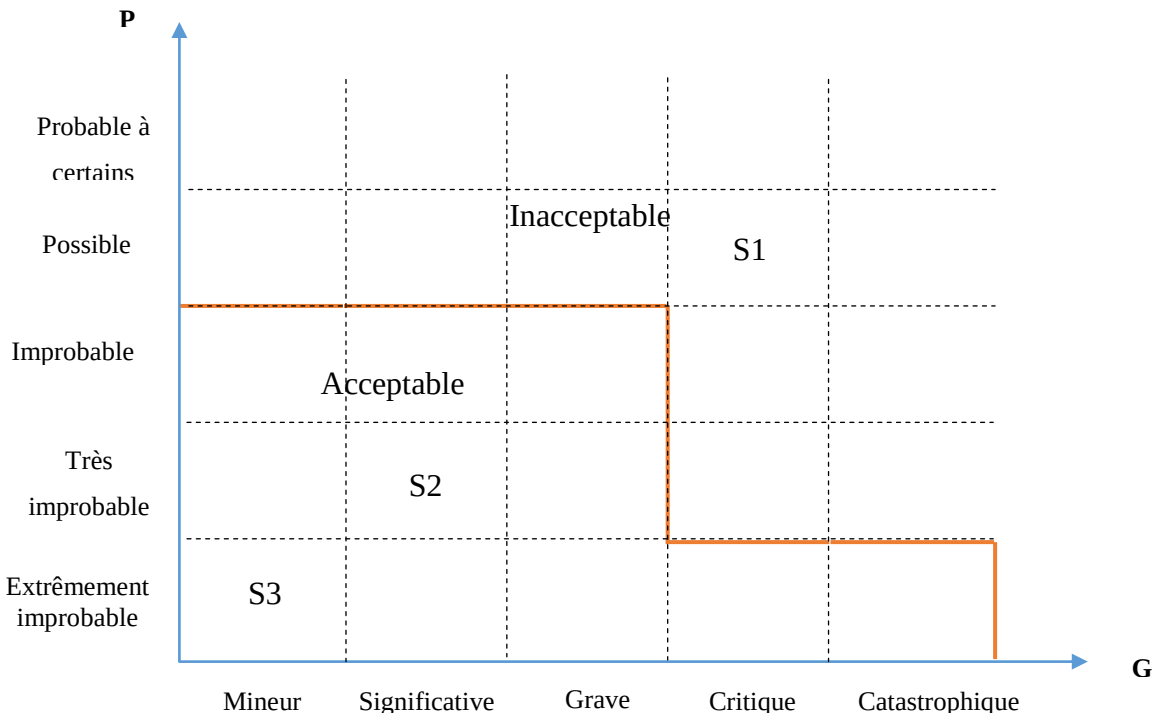
Nous allons en premier lieu, classer nos scénarios longs retenus dans chaque sous-système dans une matrice (figures 16, 17, 18, 19). Ensuite nous allons classer les scénarios dans les quatre tableaux cités qui suit (tableaux 02, 03, 04, 05 : échelle de gravité générique ; tableaux 06, 07, 08, 09 : échelle de vraisemblance générique), le but de ce travail et d'analyser les informations et d'attribuer à chaque scénario identifié un niveau de risque.



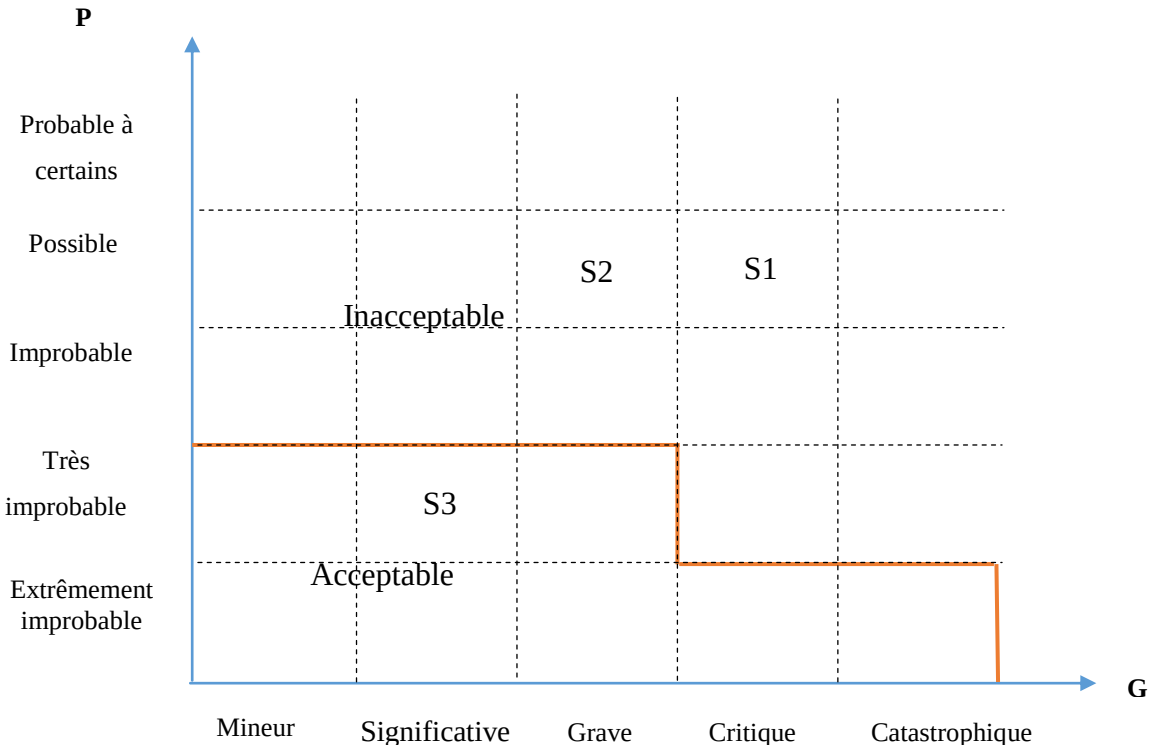
Échelle de Gravité * la Probabilité pour le SS1 Equipement



Échelle de Gravité * la Probabilité pour le SS2 Organisation



Échelle de Gravité * la Probabilité pour le SS3 Milieu



Échelle de Gravité * la Probabilité pour le SS4 Resource Humain

➢ Tableaux d'échelle de gravité des scénarios des sous-systèmes :

➢ Tableau propre au sous-système 1 :

Scénario	Classe de gravité	Intitulé des gravitées	Intitulé des conséquences
	G1	Mineur	Faire impact ne remet pas en cause les objectifs du sous-système en termes de performance et sécurité.
3	**G2**	Significative	Dégradation du niveau de performance sans impact sur l'intégrité du sous-système.
1	**G3**	Grave*	Forte à très forte dégradation du niveau de performance pouvant aller jusqu'à l'échec de la mission du sous-système, sans impact sur l'intégrité du sous-système.
2	**G4**	Critique	Dégradation de l'intégrité du sous-système
	G5	Catastrophique	Très forte dégradation de l'intégrité du sous-système pouvant aller jusqu'à sa perte

échelle de Gravité des scénarios dans le SS1 Équipement

➢ Tableau propre au sous-système 2:

Scénario	Classe de gravité	Intitulé des gravitées	Intitulé des conséquences
	G1	Mineur	Faire impact ne remet pas en cause les objectifs du sous-système en termes de performance et sécurité.
2 &3	**G2**	Significative	Dégradation du niveau de performance sans impact sur l'intégrité du sous-système.
	G3	Grave*	Forte à très forte dégradation du niveau de performance pouvant aller jusqu'à l'échec de la mission du sous-système, sans impact sur l'intégrité du sous-système.
1	**G4**	Critique	Dégradation de l'intégrité du sous-système
	G5	Catastrophique	Très forte dégradation de l'intégrité du sous-système pouvant aller jusqu'à sa perte

échelle de Gravité des scénarios dans le SS2 Organisation

- **Tableau propre au sous-système 3 :**

Scénario	Classe de gravité	Intitulé des gravitées	Intitulé des conséquences
3	G1	Mineur	Faire impact ne remet pas en cause les objectifs du sous-système en termes de performance et sécurité.
2	G2	Significative	Dégradation du niveau de performance sans impact sur l'intégrité du sous-système.
	G3	Grave*	Forte à très forte dégradation du niveau de performance pouvant aller jusqu'à l'échec de la mission du sous-système, sans impact sur l'intégrité du sous-système.
1	G4	Critique	Dégradation de l'intégrité du sous-système
	G5	Catastrophique	Très forte dégradation de l'intégrité du sous-système pouvant aller jusqu'à sa perte

Tableau 2: échelle de Gravité des scénarios dans le SS3 Milieu

- **Tableau propre au sous-système4 :**

Scénario	Classe de gravité	Intitulé des gravitées	Intitulé des conséquences
	G1	Mineur	Faire impact ne remet pas en cause les objectifs du sous-système en termes de performance et sécurité.
3	G2	Significative	Dégradation du niveau de performance sans impact sur l'intégrité du sous-système.
2	G3	Grave*	Forte à très forte dégradation du niveau de performance pouvant aller jusqu'à l'échec de la mission du sous-système, sans impact sur l'intégrité du sous-système.
1	G4	Critique	Dégradation de l'intégrité du sous-système
	G5	Catastrophique	Très forte dégradation de l'intégrité du sous-système pouvant aller jusqu'à sa perte

Tableau 3: échelle de Gravité des scénarios dans le SS4 Ressource Humain

➢ Tableaux d'échelle de vraisemblance générique des sous-systèmes :

➢ Tableau propre au sous-système 1 :

Scénario	Classes de vraisemblance	Intitulé de vraisemblance
	V1	Extrêmement improbable
	V2	Très improbable
S3	V3	Improbable
S1	V4	Possible
S2	V5	Probable à certains

Tableau 4: échelle de vraisemblance générique des scénarios dans le SS1

➢ Tableau propre au sous-système 2 :

Scénario	Classes de vraisemblance	Intitulé de vraisemblance
S3	V1	Extrêmement improbable
S2	V2	Très improbable
	V3	Improbable
S1	V4	Possible
	V5	Probable à certains

Tableau 5: échelle de vraisemblance générique des scénarios dans le SS2

➢ Tableau propre au sous-système 3 :

Scénario	Classes de vraisemblance	Intitulé de vraisemblance
S3	V1	Extrêmement improbable
S2	V2	Très improbable
	V3	Improbable
S1	V4	Possible
	V5	Probable à certains

Échelle de vraisemblance générique des scénarios dans le SS3

Tableau propre au sous-système 4 :

Scénario	Classes de vraisemblance	Intitulé de vraisemblance
	V1	Extrêmement improbable
S3	V2	Très improbable
	V3	Improbable
S1 & S2	V4	Possible
	V5	Probable à certains

Échelle de vraisemblance générique des scénarios dans le SS4

5. Définition et qualification des moyens de prévention et de protection :

Comme nous avons indiqué au paravent le traitement des risques implique le choix et la mise en œuvre d'une ou de plusieurs options de modification des scénarios dite dans le contexte de management des risques l'identification ces barrières de sécurité. La mise en œuvre de ces barrière de prévention et de protection nécessite un ensemble de mesures à prendre pour maîtriser les risques prévus dans chaque scénario retenu.

Le traitement des scénarios implique un processus itératif :

- Évaluer un traitement du scénario ;
- Décider si les niveaux de scénarios résiduels sont tolérables ;
- S'ils ne sont pas tolérables, générer un nouveau traitement du scénario; et apprécier l'efficacité de ce traitement.

Dans notre étude, nous avons fixé un seuil de gravité qui nous permettra de décider par la suite si les niveaux des scénarios résiduels sont tolérables ou non.

Ce traitement ou ces barrières de sécurité vont permettre de neutraliser les scénarios identifiés, dans ce cas-là, il suffit de neutraliser les événements primaires qui engendrent les événements principaux non souhaités.

5.1. Les barrières de sécurité suggérer :

Les barrières de sécurité, c'est des actions à mener en vue de réduire la probabilité et l'impact des risques.

Dans notre travail et sur la base des informations fournis par les responsables et les employés à travers les entretiens et les observations ainsi les documents de la direction mise à notre disposition, nous avons défini les barrières de sécurité comme recommandations aux dirigeants notamment les sous-directions afin d'optimiser le processus de gestion des risques de la Direction Informatique.

5.2.1. La communication et la sensibilisation :

En regard à l'importance de la communication horizontale et verticale dans la démarche de gestion des risques au sein d'un organisme, il est fortement recommandé à la direction informatique d'instaurer une stratégie de communication au tour des risques qui peuvent affecter le système informatique.

La en place d'un programme de sensibilisation continu par la direction représente aussi une démarche efficace pour augmenter le niveau de la vigilance chez les employés de façon

que tout le monde soit conscient vis-à-vis de la sécurité interne de système informatique de la direction.

5.2.2. La coordination :

L'absence de la coordination entre les différents sous-direction et la direction informatique peut causer certainement un dysfonctionnement au niveau du système d'informatique quelle que soit leur efficacité, ce qui implique la présence d'une culture organisationnelle d'échange d'informations liées à l'aspect sécurité entre les différents sous-direction et la direction informatique peut participer fortement dans le processus de management des risques envisagés dans les scénarios imaginés pour un système informatique.

5.2.3. La formation :

Il est recommandé à la direction informatique d'élaborer un programme de formation continue au profit de l'ensemble des employés au niveau des sous-directions des systèmes informatiques en vue d'acquérir le savoir-faire et savoir être vis-à-vis à la sécurité du système informatique et le rôle de chaque employé dans le processus de management des risques dans DI.

5.2.4. Promouvoir une culture de sécurité contre le risque informatique au sein de la direction :

D'après notre interprétation des résultats des entretiens, on remarque la majorité des répondants ne savent pas que chaque membre de l'organisation de la direction est le maillon fort dans la sécurité contre le risque informatique. Pour cela il est fortement recommandé à la direction de mettre à la disposition de l'ensemble des employés des documentations et affiches ainsi que de mener des actions de formation afin de renforcer la culture de sécurité contre le risque dans le système informatique et qui rendre la réflexion chez les employés plus efficace afin de signaler par exemple toute anomalie qui peut affecter la sécurité de système informatique aux responsables de la DI.

5.2.5. Surveillance et revue :

L'avancement de la mise en œuvre des plans de traitement des risques constitue une mesure de la performance de la DI. Les résultats peuvent être intégrés au management global des performances de l'organisme, à leur mesurage et aux activités d'élaboration de rapports externes et internes.

Il convient que les résultats de la surveillance et de la revue soient enregistrés, fassent l'objet de rapports internes et externes selon les besoins, et servent à donner à la revue du cadre organisationnel de gestion du risque dans la DI.

5.2.6. Enregistrement du processus :

Il convient que les activités de management du risque puissent être tracées. Dans le processus de management du risque, les enregistrements fournissent la base de l'amélioration des méthodes et des outils ainsi que du processus dans son ensemble.

Il convient que les décisions des responsables du système informatique de la DI relatives à la création des enregistrements des informations relatives à la sécurité contre les risques informatiques dans la DI prennent en compte :

- les besoins de l'organisme en matière d'acquisition continue de connaissances,
- les avantages de la réutilisation d'informations pour répondre à des objectifs de management,
- les coûts et le travail liés à la création et à la maintenance des enregistrements,
- les nécessités légales, réglementaires et opérationnelles d'effectuer des enregistrements,
- la méthode d'accès, la facilité de consultation et les moyens de stockage,
- la période de conservation, et le caractère sensible des informations.

CONCLUSION

L‘application de la méthode MADS-MOSAR pour assurer une meilleur gestion prospective de risque informatiques au sien de la direction informatique nous a permet d‘identifier quelques scénarios de risques et d‘établir des barrières que nous pensons adéquates en vue d‘éliminer les systèmes sources de dangers mais non suffisante. Il apparaît clairement que dans ce parcours, analyser les risques ; consiste à identifier, évaluer, maîtriser, manager et gérer ces derniers.

L‘établissement de barrières ne veux nullement dire que nous sommes dans un scénario de risque zéro, le déroulement d‘un événement non souhaité (incendie, perte, débordement…etc.) N‘est jamais acquise dans un système informatiques d’une direction d‘où la nécessité d‘élaborer un plan d‘organisation interne et d‘un plan particulier d‘intervention.

Globalement, nous pouvons dire que MADS-MOSAR est une bonne méthode d’analyse de risque. En effet, si elle a été essentiellement créée pour des applications dans le monde de l’industrie, elle n’en reste pas moins parfaitement transposable à ce domaine.

Par conséquent, les faiblesses et les points forts de l’analyse des risques dans le domaine de l’industrie sont les mêmes que pour tout autre domaine. Le point négatif de la méthode est qu’elle ne nous dit pas si notre liste de scénarios ou de source de danger est complète. Par conséquent, nous avons en permanence une liste non exhaustive d’évènements, ce qui peut amener à oublier certains risques. Mis à part cet aspect, la méthode MADS-MOSAR s’utilise très facilement. De plus, et cela est très intéressant pour notre étude mais aussi pour d’autres, elle est extrêmement flexible et s’adapte très bien à divers domaines.

Nous pensons que dans le futur, il faudra compléter cette étude en recherchant de nouveaux scénarios de risque, de nouvelles sources de danger et de nouvelles barrières. On pourra bien entendu réaliser le module B de la méthode, c’est à dire l’approche microscopique.

L’approche rigoureuse développée ci-dessus a pour objectif de faire (ou de refaire) un inventaire exhaustif de tous les risques présents dans les installations avec pour chaqu’un d’eux la possibilité de vérifier qu’une maîtrise en est assurée et surtout que les risques majeurs sont ramenés à un risque acceptable. Elle permet de s’assurer de façon rigoureuse qu’un lien avec le système de management de la sécurité a bien été fait notamment pour la gestion rigoureuse des barrières mises en place.

En conclusion, il y a lieu de souligner que nous vivons encore dans le paradigme hérité des années passées d'un système conduit par des opérateurs de proximité (de première ligne) responsables du comportement final de l'ensemble homme - machine. Néanmoins celui-ci

s'est optimisé au fil des ans, en franchissant différentes barrières (travail en ambiances nocives, travail de nuit, travail sur écrans, conduite à distance, aides automatisées, etc.). Par ailleurs, les solutions techniques ont améliorés mais en augmentant progressivement la complexité du système, et cette complexité est devenue le point limitant l'action du facteur humain. Celui-ci doit s'adapter aux exigences de la complexification des systèmes sociotechniques. Son rôle étant capital dans l'évitement des dérives accidentelles ou intentionnelles, prévisibles ou imprévisibles à caractère risque mineur ou majeur.

Les solutions existent potentiellement, mais elles demandent une éducation des différents acteurs aux risques et un changement conséquent de mentalité à tous les niveaux de la hiérarchie. Il s'agit de repenser la relation entre la technique et l'homme dans le dialogue des disciplines. Il s'agit d'entamer une logique d'intégration, de confrontation, une mise en tension permanente dans un esprit constructif.

Il est admis quand la technique et l'homme doivent s'assembler, la résultante est irréductiblement hétérogène. Même si la part intégrable de l'homme progresse de pair avec la connaissance, elle n'en demeure pas moins marginale en regard de sa globalité : « *l'homme ne peut être appréhendé sous forme de facteur, il est l'acteur et l'acteur principal* ».

RÉFÉRENCES BILIOGRAPHIQUES

OUVRAGES

- Angers Maurice. (1999) Initiation pratique à la méthodologie des sciences humaines. Casbah, Alger, p09, p146, p129.
- BARTHELEMY Bernard (2004), Gestion des risques : méthode d'optimisation globale, Editions d'Organisation, Paris, p87, p72.
- CALE.S, Philippe Touitou (2007), Sécurité Informatique, Editions Lavoisier, Paris, p57, p43, p44, p55, p66.
- CLAUDE Pinet (2012), 10 clés pour la sécurité de l'information : ISO/CEI 27001, Editions AFNOR, Paris, p39, (p41-42).
- DEYRIEUX André (2003), le système d'information : nouvel outils de stratégie, direction d'entreprise et direction du système d'information, Editions Maxima, Paris, p10, p11.
- DELMOND Marie-Hélène, PETIT Yves et GAUTIER Jean-Michel (2008), Management des systèmes d'information, 2ème édition, Editions Dunod, Paris, p112, p113.
- DAYAN Armand (2008), Manuel de gestion, vol.1, 2ème édition, Editions Ellipses/AUF, Paris, p1075.
- DARSA Jean-David (2013), Les risques opérationnels de l'entreprise : un environnement toujours plus risqué ?, Editions Gereso, Paris, p218.
- DELEUZE Gilles (2013), Analyse des risques : concepts, outils, gestion, maîtrise, Editions EMS, Paris, p299.
- DESROCHES Alain, LEROY Alain, et VALLEE Frédérique (2007), La gestion des risques, 2ème édition, Editions Lavoisier, Paris, p209.
- GREUNING Hennie Van et BRATANOVIC Sonja Barjovic (2004), Analyse et gestion du risque bancaire, Editions ESKA, Paris, p33.
- Gordon. M. et Petry.F. (2000) Guide d'élaboration d'un projet de recherche en sciences sociales. 4eme édition, Deboeck, Canada, p41.
- Grawitz Madeline. Méthodes des sciences sociales. 11eme édition, Dalloz, p351, 352.
- GRAEVE Jean de et POTIER Jean (2001), Système d'information, Management et Acteurs, Editions Sapienta, Paris, p03.
- HERVE Fratta, MADERS Henri- Pierre et MASSELIN Jean-Luc (2014), Les métiers d'auditeur interne et de contrôleur permanent, Editions Eyrolles, Paris, p06.
- JEAN LE REY, (2010), Gérer les risques, Pourquoi ? Comment ? Ed. AFNOR, Paris, p32.
- JEAN Le Ray, Gérer les risques, Pourquoi ? Comment ? Afnor Editions, 2006, 392 pages.
- Loubet, DELBAYLE (Jean Louis). Initiation aux méthodes des sciences sociales. L'Harmation, Paris, p61.
- LAUDON Jane et LAUDON Kenneth (2011), Management des systèmes d'information,
- MONACO Laurence (2014), Les carrés DCG 8 : Système d'information de gestion 2014-2015, Editions Guialino, Paris, p17, p18.
- Michel Godet, (2007), Manuel de Prospective Stratégique, Tome 1, une indiscipline intellectuelle, chapitre 1 -Le rêve féconde la réalité, Editions Dunod, Paris, p11.

- O'BRIEN James (1995), Les système d'information de gestion, Editions du Renouveau Pédagogique, Montréal, p19.
- OLIVIER GRANDAMAS5 (2012) « Méthode MADS-MOSAR - Pour en favoriser la mise en oeuvre », Techniques de l'Ingénieur [se4062], (France).
- PILLOU Jean-François et CAILLEREZ Pascal (2011), Tout sur les systèmes d'information Grandes, moyennes et petites entreprises, 2ème édition, Editions Dunod, Paris, p81, p23.
- Pascal Kerebel, 2009, Management des risques, secteur banque et assurance, Ed. Eyrolles, 187 pages.
- Patrick Lagadec,(1991), Gestion de crise, outils de réflexion à l'usage des décideurs, MCGRAW-HILL, 300 pages.
- PIERRE PERILHON (2012) *« MOSAR-Présentation de la méthode »*, Techniques de
- l'Ingénieur [se4060], (France).
- Patrick Lagadec, 1988, Etats d'Urgence, Seuil, 405 pages.
- Patrick Lagadec, 1981, La civilisation du risque, Seuil.
- Romain Laufer, 1993, L'entreprise face aux risques majeurs, à propos de l'incertitude des normes sociales (Logiques sociales-L'Harmattan), 319 pages.
- REIX Robert, FALLERY Bernard et KALIKA Michel (2011), Système d'information et management des risques, 6ème édition, Editions Vuibert, Paris, p04, p05.
- RENARD Jacques (2010), Théorie et Pratique de l'Audit Interne, 7ème édition, Editions d'Organisation, Paris, p155.
- SATZINGER John W, JACKSON Robert B et BURD Stephen D (2003), Analyse et conception de systèmes d'information, 2ème édition, Editions Renard Goulet, Paris, p08.
- Sean Cleary, Thierry Malleret, 2006, Risques : Perception, Evaluation, Gestion, Editions Maxima 249 pages.
- VOLLE Michel (2004), Lexique du système d'information, Club des maitres d'ouvrage des systèmes d'information & Michel VOLLE, Editions GNU Free Documentations, Paris, p11.

Revues et articles :

- Futuribles n°354-juillet-août 2009, Vers l'apocalypse ? Gérard Donnadieu.
- Business Digest, collection Les états de l'art, n°117, mars 2002, La prospective, Art ou discipline ?
- MUNOZ.F, PERRIN.L, SARDIN.M, JOSIEN.J.P. (2006).The approach. MADS/MOSAR.to manage the triptych "technology / normative /management». Society for Risk Analysis Europe 15th Annual Conference. Ljubljana, Slovénie11, 13 Septembre2006.
- La Tribune, 26 janvier 2006, Frédéric Hastings, « le Risk Manager s'installe dans une approche globale des risques ».
- BAPST Pierre Alexandre, BERGERET Florence (2002), Pour un management des risques orienté vers la protection de l'entreprise et la création de la valeur ajoutée (deuxième partie), Revue française de l'audit interne, N°162 : 31-33.
- Les Echos, dossiers L'Art de la gestion des risques.

-La quête de la sécurité dans un monde fluctuant. Gregory W.Brown.
-Peur du risque…ou de l'innovation ? Christoph H.Loch et ArndHuchzermeier.

- Le Figaro, article du 23/07/2010, « La Chine confrontée à une terrible marée noire. » http://www.lefigaro.fr/international/2010/07/23/01003 -20100723ARTFIG00503-la-chine-confrontee- a-une-terrible-maree-noire.php
- Revue Risk&Insurance, 15 avril 2004, (Etude sur les risques, types de risques importants pouvant impacter les économies développées.)
- Revue Educnet, Economie & gestion, rubrique Systèmes d'information, Sécurité des systèmes d'information : de la gestion des risques à la confiance numérique.

Site Web :

- CIGREF (2009), Les référentiels de la DSI, http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2009/Referentiels_de_la_DSI_CIGREF_2009.pdf, p120.
- NIST (2002),*Risk Management guide for IT*,http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30
- AMRAE-CLUSIF(2006), RM et RSSI: Deux métiers qui s'unissent pour la gestion des risques liés au système d'information, https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf, p04.
- www.rms.com ; http://www.rms.com/AboutRMS/Expertise/Research.asp
- http://www.inventive-design.net/content/view/242/1/
- http://www.rffst.org/images/6/60/Fiche_Double_approche_systemique_pluridisciplinaire_RFFST.pdf

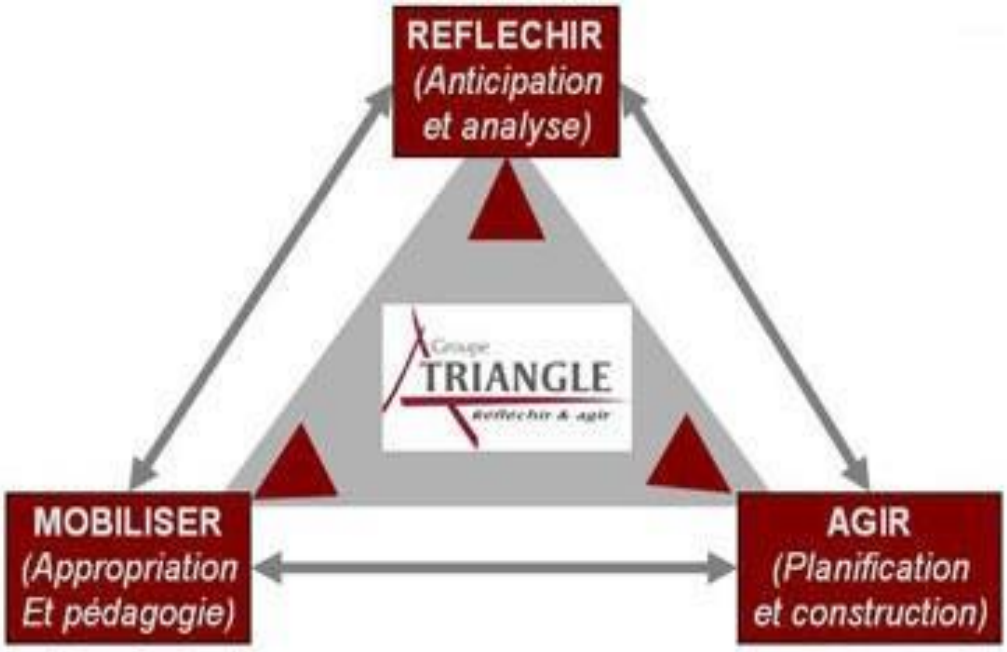
ANNEXE I –LES TYPES DE RISQUES INFORMATIQUES

	Arrêt de maintenance de logiciels par disparition de la SSII/ du fournisseur concepteur de la solution
	Divulgation des données confidentielles
	Accidents naturels
	Vandalisme sur équipement sans intrusion
	Vandalisme sur équipement avec intrusion dans les locaux
	Vol d'équipement avec intrusion dans les locaux
	Vol d'équipement sans intrusion
	Dégâts des eaux ou autre liquide
	Vol d'information (sensible ou non)
	Vol d'information et diffusion au public
	Destruction volontaire d'information
	Modification volontaire d'information
	Altération volontaire d'information
	Intrusion dans les systèmes
	Perturbation des services rendus
	Détournement d'un site, d'un service vendu (site web, contact email etc.)
	Ecoute d'information sur le réseau (intrusion réseau interne)
	Altération accidentelles des informations par l'exploitation (perte ou dégradation des données)
	Abus de pouvoir par une maintenance externe (TMA, mainteneur outrepassant droits
	Dysfonctionnement d'un matériel (panne physique)
	Dysfonctionnement d'un logiciel (panne logique)

	Dysfonctionnement d'un service externe (perte de compétence d'un tiers)
	Blocage centre informatique ou locaux métiers
	Erreur de saisie (erreur manuelle, création d'anomalie,
	Virus informatiques (attaques virale)
	Absence de données critiques (perte de données sensibles particulières)

Source : Nous-mêmes à partir de DARSA (2014)

ANNEXE II – LE TRIANGLE GREC



(Source, Groupe Triangle Grec)

ANNEXE III – EXEMPLE DE CARTOGRAPHIE DES RISQUES

Source Digimind Redbook Risk Management-2010.

ANNEXE IV – GUIDE D'ENTRETIEN

Guide d'entretien

L'objectif de ce guide d'entretien est de pouvoir évaluer l'efficacité de la méthode MADS –MOSAR afin d'assurer une meilleur gestion des risques au sien de la Direction Informatique de la DGB.

➢ Axe 1 : Système informatique dans la direction

1) Pouvez-vous nous faire une description synoptique de l'activité de votre service ?

2) Parlez-moi du système informatique de la direction ?

3) Existe-t-il une coordination entre les travaux du service informatique et ceux d'autres services de la direction générale ?

4) Existe-t-il une charte informatique ? Est-elle est régulièrement mise à jour ?

5) Existe-t-il une politique informatique ? Est-elle régulièrement mise à jour?

6) Existe-t-il une politique de sécurité informatique?

7) Est-ce qu'il existe une procédure de sauvegarde des données clairement définie ?

➢ Axe 2 : Dispositif de gestion des risques informatiques dans la direction

6) Est-ce une cellule de gestion de risque informatique existe-t-elle dans la direction ?

7) Qui est le gestionnaire des risques informatiques ?

8) Pouvez-vous nous faire une description la méthodologie de gestion des risques ?

9) Disposez-vous d'une cartographie des risques ?

10) Pour quelles méthodes avez-vous optée dans le cadre de la gestion des risques informatiques?

11) Quels sont les objectifs du dispositif de maîtrise des risques informatiques ?

12) Quels sont les sous-systèmes source de danger dans la direction ?

13) Quelles sont les principaux risques que vous rencontrez souvent dans le système informatique de la direction ?

14) Le personnel est-il impliqué dans le processus identification des risques ? Et est ce qu'il est suffisant ?

15) Le personnel est-il doté de qualification et d'une expérience en maitrise de risque informatique ?

16) Existe-t-il un programme de communication et de sensibilisation aux risques informatiques ?

17) Considérez-vous que l'équipe informatique dispose d'une compétence suffisante en matière de gestion et maîtrise des risques informatiques pour pouvoir s'acquitter de manière efficace de cette tâche ?